

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-359616

(P2002-359616A)

(43) 公開日 平成14年12月13日 (2002. 12. 13)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード(参考)
H 0 4 L 9/08		G 0 9 C 5/00	5 J 1 0 4
G 0 9 C 5/00		H 0 4 L 9/00	Z E C
H 0 4 L 9/00	Z E C		6 0 1 B
9/32			6 7 5 B

審査請求 未請求 請求項の数14 O L (全 35 頁)

(21) 出願番号 特願2002-28915(P2002-28915)

(22) 出願日 平成14年2月6日(2002. 2. 6)

(31) 優先権主張番号 特願2001-33114(P2001-33114)

(32) 優先日 平成13年2月9日(2001. 2. 9)

(33) 優先権主張国 日本 (J P)

(31) 優先権主張番号 特願2001-94803(P2001-94803)

(32) 優先日 平成13年3月29日(2001. 3. 29)

(33) 優先権主張国 日本 (J P)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 田中 浩一

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72) 発明者 河上 達

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74) 代理人 100082131

弁理士 稲本 義雄

最終頁に続く

(54) 【発明の名称】 情報処理装置および方法、ライセンスサーバ、並びにプログラム

(57) 【要約】

【課題】 コンテンツの配布を自由に行うことができ、許可されたユーザのみがコンテンツを利用できるようにする。

【解決手段】 クライアントは暗号化されたコンテンツをコンテンツサーバから受け取る。コンテンツのヘッダにはそのコンテンツを利用するとき必要とされるライセンスを特定するためのライセンス特定情報が記述されており、クライアントはライセンス特定情報を元にライセンスサーバにライセンスを要求する。ライセンスサーバは、ライセンス要求を受け取ると、課金処理を行った後、該当するライセンスをクライアントに送信する。クライアントはライセンスを保持していることを条件として、コンテンツを復号し再生する。

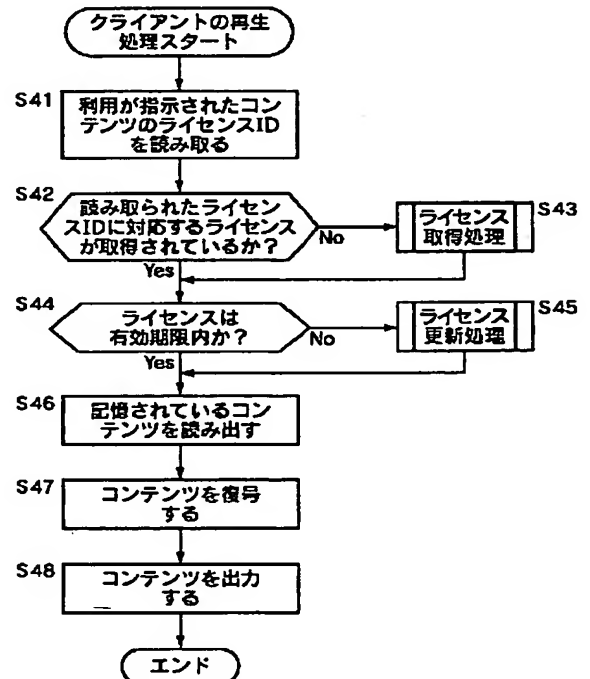


図6

## 【特許請求の範囲】

【請求項1】 ライセンスを保持していることを条件としてコンテンツの利用を許可する情報処理装置において、

当該コンテンツを利用許可する前記ライセンスを特定するためのライセンス特定情報と、暗号化されたコンテンツデータと、コンテンツデータを復号するために必要な鍵情報とを含む前記コンテンツを記憶するコンテンツ記憶手段と、

利用許可される前記コンテンツを特定するためのコンテンツ特定情報を含むライセンスを記憶するライセンス記憶手段と、前記コンテンツを利用許可することができるライセンスが前記ライセンス記憶手段に記憶されているか否かを判定する判定手段と、

前記判定手段によりライセンスが記憶されていると判断されたことを条件として前記コンテンツのコンテンツデータを復号する復号手段とを備えることを特徴とする情報処理装置。

【請求項2】 前記情報処理装置は更に、ライセンスサーバにライセンスを識別するためのライセンス識別情報を含むライセンス要求を送信する送信手段と、

ライセンスサーバによって送信されたライセンスを受信する受信手段とを備え、

前記受信手段により受信されたライセンスは前記ライセンス記憶手段に記憶されることを特徴とする請求項1記載の情報処理装置。

【請求項3】 前記コンテンツデータはテキストデータ、画像データ、音声データ、動画データあるいはそれらを組み合わせたデータであり、

前記復号手段により復号されたコンテンツデータを再生する再生手段を更に備えることを特徴とする請求項1記載の情報処理装置。

【請求項4】 前記鍵情報はEKB (Enabling Key Block) を含み、

前記情報処理装置は更にデバイスノードキーを記憶するデバイスノードキー記憶手段を備え、

前記復号手段は前記デバイスノードキー記憶手段に記憶されている前記デバイスノードキーを用いて前記EKB (Enabling Key Block) を復号処理し得られたルートキーを用いて前記暗号化されたコンテンツデータを復号することを特徴とする請求項1記載の情報処理装置。

【請求項5】 前記鍵情報は更に前記EKB (Enabling Key Block) のルートキーによって暗号化されたコンテンツキーを含み、

前記コンテンツデータは前記コンテンツキーにより暗号化されており、

前記復号手段は前記デバイスノードキー記憶手段に記憶されている前記デバイスノードキーを用いて前記EKB (Enabling Key Block) を復号処理し得られたルートキー

を用いて復号された前記コンテンツキーを用いて前記暗号化されたコンテンツデータを復号することを特徴とする請求項4記載の情報処理装置。

【請求項6】 前記ライセンスは更に、当該ライセンスによって利用可能となるコンテンツの使用条件を示す使用条件情報を含むことを特徴とする請求項1記載の情報処理装置。

【請求項7】 前記ライセンスは更に、ライセンスサーバの秘密鍵によりなされた電子署名を含むことを特徴とする請求項1記載の情報処理装置。

【請求項8】 前記情報処理装置は、更に情報処理装置を識別する端末識別情報を記憶する端末識別情報記憶手段を備え、前記ライセンス要求は更に、端末識別情報記憶手段に記憶されている前記端末識別情報を含み、前記受信手段により受信された前記ライセンスは更に、前記端末識別情報を含み、

前記判定手段は、前記ライセンスに含まれる前記端末識別情報と前記端末識別情報記憶手段に記憶されている前記端末識別情報とを比較し、両者が一致している場合に限り、当該ライセンスを前記コンテンツの利用を許可できるライセンスであると判定することを特徴とする請求項2記載の情報処理装置。

【請求項9】 ライセンスを保持していることを条件としてコンテンツの利用を許可する情報処理方法であって、

当該コンテンツを利用許可する前記ライセンスを特定するためのライセンス特定情報と、暗号化されたコンテンツデータと、コンテンツデータを復号するために必要な鍵情報と、を含むコンテンツを記憶するステップと、

当該ライセンスによって利用許可される前記コンテンツを特定するためのコンテンツ特定情報を含むライセンスを記憶するステップと、

前記コンテンツを利用許可することができるライセンスが前記ライセンス記憶手段に記憶されているか否かを判定するステップと、

前記判定手段によりライセンスが記憶されていると判断されたことを条件として前記コンテンツのコンテンツデータを復号するステップとを含むことを特徴とする情報処理方法。

【請求項10】 ライセンスを保持していることを条件としてコンテンツの利用を許可する処理をコンピュータに実行させるプログラムであって、

当該コンテンツを利用許可する前記ライセンスを特定するためのライセンス特定情報と、暗号化されたコンテンツデータと、コンテンツデータを復号するために必要な鍵情報と、を含むコンテンツを記憶するステップと、

当該ライセンスによって利用許可される前記コンテンツを特定するためのコンテンツ特定情報を含むライセンスを記憶するステップと、

前記コンテンツを利用許可することができるライセンス

が前記ライセンス記憶手段に記憶されているか否かを判定するステップと、  
前記判定手段によりライセンスが記憶されていると判断されたことを条件として前記コンテンツのコンテンツデータを復号するステップとをコンピュータに実行させるプログラム。

【請求項11】 前記プログラムあるいはその一部が暗号化されていることを特徴とする請求項10記載のプログラム。

【請求項12】 コンテンツの利用を許可するライセンスを発行するライセンスサーバにおいて、  
当該ライセンスによって利用許可される前記コンテンツを特定するためのコンテンツ特定情報と、情報処理装置を識別する端末識別情報を含む前記ライセンスを記憶するライセンス記憶手段と情報処理装置から送信された、ライセンスを識別するライセンス識別情報を含むライセンス要求を受信する受信手段と、  
前記ライセンス要求に含まれる前記ライセンス識別情報に対応する前記ライセンスを前記ライセンス記憶手段から抽出する抽出手段と、  
前記抽出手段により抽出された前記ライセンスに前記端末識別情報を付加する処理手段と、  
ライセンスサーバの秘密鍵を用いて、前記処理手段により端末識別情報を付加されたライセンスに電子署名を付加する署名手段と、  
前記署名手段により署名されたライセンスを前記ライセンス要求を送信した情報処理装置に送信する送信手段とを備えることを特徴とするライセンスサーバ。

【請求項13】 コンテンツの利用を許可するライセンスを発行する情報処理方法であって、  
当該ライセンスによって利用許可される前記コンテンツを特定するためのコンテンツ特定情報と、情報処理装置を識別する端末識別情報を含む前記ライセンスを記憶するステップと、  
情報処理装置から送信された、ライセンスを識別するライセンス識別情報を含むライセンス要求を受信するステップと、  
前記ライセンス要求に含まれる前記ライセンス識別情報に対応する前記ライセンスを前記ライセンス記憶手段から抽出するステップと、  
前記抽出手段により抽出された前記ライセンスに前記端末識別情報を付加するステップと、  
ライセンスサーバの秘密鍵を用いて、前記処理手段により端末識別情報を付加されたライセンスに電子署名を付加するステップと、  
前記署名手段により署名されたライセンスを前記ライセンス要求を送信した情報処理装置に送信するステップとを含むことを特徴とする情報処理方法。

【請求項14】 コンテンツの利用を許可するライセンスを発行する処理処理をコンピュータに実行させるプロ

グラムであって、

当該ライセンスによって利用許可される前記コンテンツを特定するためのコンテンツ特定情報と、情報処理装置を識別する端末識別情報を含む前記ライセンスを記憶するステップと、

情報処理装置から送信された、ライセンスを識別するライセンス識別情報を含むライセンス要求を受信するステップと、

前記ライセンス要求に含まれる前記ライセンス識別情報に対応する前記ライセンスを前記ライセンス記憶手段から抽出するステップと、

前記抽出手段により抽出された前記ライセンスに前記端末識別情報を付加するステップと、

ライセンスサーバの秘密鍵を用いて、前記処理手段により端末識別情報を付加されたライセンスに電子署名を付加するステップと、

前記署名手段により署名されたライセンスを前記ライセンス要求を送信した情報処理装置に送信するステップとをコンピュータに実行させるプログラム。

## 20 【発明の詳細な説明】

### 【0001】

【発明の属する技術分野】本発明は、情報処理装置および方法、ライセンスサーバ、並びにプログラムに関し、特に、著作権者からライセンスを受けていないコンテンツが不正にコピーされ、利用されるのを防止することができるようにした、情報処理装置および方法、ライセンスサーバ、並びにプログラムに関する。

### 【0002】

【従来の技術】最近、インターネットを介して、ユーザが、自分自身が保持している音楽データを他のユーザに提供し、自分自身が保持していない音楽データを他のユーザから提供を受けるようにして、複数のユーザが無料で音楽データを交換しあうシステムが実現されている。

【0003】このようなシステムでは、理論的には、1つの音楽、その他のコンテンツが存在すれば、他の全てのユーザが、それを利用することが可能となり、多くのユーザがコンテンツを購入しなくなるため、コンテンツに関する著作権者は、著作物としてのコンテンツが売れないため、著作物の販売に伴い、本来受け取ることが可能な著作物の利用に関するロイヤリティを受け取る機会を失うことになる。

### 【0004】

【発明が解決しようとする課題】そこで、コンテンツの流通を妨げることなく、不正に利用されることを防止することが、社会的に要請されている。

【0005】本発明はこのような状況に鑑みてなされたものであり、コンテンツが不正に利用されるのを確実に防止することができるようにするものである。

### 【0006】

【課題を解決するための手段】本発明の情報処理装置

は、コンテンツを利用許可するために必要なライセンスを特定するためのライセンス特定情報と、暗号化されたコンテンツデータと、コンテンツデータを復号するために必要な鍵情報とを含むコンテンツを記憶するコンテンツ記憶手段と、利用許可されるコンテンツを特定するためのコンテンツ特定情報を含むライセンスを記憶するライセンス記憶手段と、コンテンツを利用許可することができるライセンスがライセンス記憶手段に記憶されているか否かを判定する判定手段と、判定手段によりライセンスが記憶されていると判断されたことを条件としてコンテンツのコンテンツデータを復号する復号手段とを備えることを特徴とする。

【0007】情報処理装置は更に、ライセンスサーバにライセンスを識別するためのライセンス識別情報を含むライセンス要求を送信する送信手段と、ライセンスサーバによって送信されたライセンスを受信する受信手段とを備え、受信手段により受信されたライセンスはライセンス記憶手段に記憶されるようにすることができる。

【0008】コンテンツデータはテキストデータ、画像データ、音声データ、動画データあるいはそれらを組み合わせたデータであり、復号手段により復号されたコンテンツデータを再生する再生手段を更に備えるようにすることができる。

【0009】鍵情報はEKB (Enabling Key Block) を含み、情報処理装置は更にデバイスノードキーを記憶するデバイスノードキー記憶手段を備え、復号手段はデバイスノードキー記憶手段に記憶されているデバイスノードキーを用いてEKB (Enabling Key Block) を復号処理し得られたルートキーを用いて暗号化されたコンテンツデータを復号するようすることができる。

【0010】鍵情報は更にEKB (Enabling Key Block) のルートキーによって暗号化されたコンテンツキーを含み、コンテンツデータはコンテンツキーにより暗号化されており、復号手段はデバイスノードキー記憶手段に記憶されているデバイスノードキーを用いてEKB (Enabling Key Block) を復号処理し得られたルートキーを用いて復号されたコンテンツキーを用いて暗号化されたコンテンツデータを復号するようすることができる。

【0011】ライセンスは更に、そのライセンスによって利用可能となるコンテンツの使用条件を示す使用条件情報を含むようすることができる。

【0012】ライセンスは更に、ライセンスサーバの秘密鍵によりなされた電子署名を含むようすることができる。

【0013】情報処理装置は、更に情報処理装置を識別する端末識別情報を記憶する端末識別情報記憶手段を備え、ライセンス要求は更に、端末識別情報記憶手段に記憶されている端末識別情報を含み、受信手段により受信されたライセンスは更に、端末識別情報を含み、判定手段は、ライセンスに含まれる端末識別情報と端末識別情

報記憶手段に記憶されている端末識別情報とを比較し、両者が一致している場合に限り、そのライセンスをコンテンツの利用を許可できるライセンスであると判定するようにすることができる。

【0014】本発明の情報処理方法は、コンテンツを利用許可するライセンスを特定するためのライセンス特定情報と、暗号化されたコンテンツデータと、コンテンツデータを復号するために必要な鍵情報と、を含むコンテンツを記憶するステップと、利用許可されるコンテンツを特定するためのコンテンツ特定情報を含むライセンスを記憶するステップと、コンテンツを利用許可することができるライセンスがライセンス記憶手段に記憶されているか否かを判定するステップと、判定手段によりライセンスが記憶されていると判断されたことを条件としてコンテンツのコンテンツデータを復号するステップとを含むことを特徴とする。

【0015】本発明のプログラムは、コンテンツを利用許可するライセンスを特定するためのライセンス特定情報と、暗号化されたコンテンツデータと、コンテンツデータを記憶するステップと、利用許可されるコンテンツを特定するためのコンテンツ特定情報を含むライセンスを記憶するステップと、コンテンツを利用許可することができるライセンスがライセンス記憶手段に記憶されているか否かを判定するステップと、判定手段によりライセンスが記憶されていると判断されたことを条件としてコンテンツのコンテンツデータを復号するステップとをコンピュータに実行させる。

【0016】プログラムあるいはその一部が暗号化されているようにすることができる。

【0017】本発明のライセンスサーバは、許可されるコンテンツを特定するためのコンテンツ特定情報と、情報処理装置を識別する端末識別情報を含むライセンスを記憶するライセンス記憶手段と、情報処理装置から送信された、ライセンスを識別するライセンス識別情報を含むライセンス要求を受信する受信手段と、ライセンス要求に含まれるライセンス識別情報に対応するライセンスをライセンス記憶手段から抽出する抽出手段と、抽出手段により抽出されたライセンスに端末識別情報を付加する処理手段と、ライセンスサーバの秘密鍵を用いて、処理手段により端末識別情報を付加されたライセンスに電子署名を付加する署名手段と、署名手段により署名されたライセンスをライセンス要求を送信した情報処理装置に送信する送信手段とを備えることを特徴とする。

【0018】本発明の情報処理方法は、利用許可されるコンテンツを特定するためのコンテンツ特定情報と、情報処理装置を識別する端末識別情報を含むライセンスを記憶するステップと、情報処理装置から送信された、ライセンスを識別するライセンス識別情報を含むライセンス要求を受信するステップと、ライセンス要求に含まれ

るライセンス識別情報に対応するライセンスをライセンス記憶手段から抽出するステップと、抽出手段により抽出されたライセンスに端末識別情報を付加するステップと、ライセンスサーバの秘密鍵を用いて、処理手段により端末識別情報を付加されたライセンスに電子署名を付加するステップと、署名手段により署名されたライセンスをライセンス要求を送信した情報処理装置に送信するステップとを含むことを特徴とする。

【0019】本発明の情報処理装置、情報処理方法、並びにプログラムでは、ライセンスを保持していることを条件としてコンテンツを復号し、利用可能にする。

【0020】本発明のライセンスサーバ、並びに情報処理方法では、特定の情報処理装置でのみ有効なライセンスを発行する。

【0021】

【発明の実施の形態】図1は、本発明を適用したコンテンツ提供システムの構成を示している。インターネット2には、クライアント1-1、1-2（以下、これらのクライアントを個々に区別する必要がある場合、単にクライアント1と称する）が接続されている。この例においては、クライアントが2台のみ示されているが、インターネット2には、任意の台数のクライアントが接続される。

【0022】また、インターネット2には、クライアント1に対してコンテンツを提供するコンテンツサーバ3、コンテンツサーバ3が提供するコンテンツを利用するのに必要なライセンスをクライアント1に対して付与するライセンスサーバ4、およびクライアント1がライセンスを受け取った場合に、そのクライアント1に対して課金処理を行う課金サーバ5が接続されている。

【0023】これらのコンテンツサーバ3、ライセンスサーバ4、および課金サーバ5も、任意の台数、インターネット2に接続される。

【0024】図2はクライアント1の構成を表している。

【0025】図2において、CPU（Central Processing Unit）21は、ROM（Read Only Memory）22に記憶されているプログラム、または記憶部28からRAM（Random Access Memory）23にロードされたプログラムに従って各種の処理を実行する。タイマ20は、計時動作を行い、時刻情報をCPU21に供給する。RAM23にはまた、CPU21が各種の処理を実行する上において必要なデータなども適宜記憶される。

【0026】暗号化復号部24は、コンテンツデータを暗号化するとともに、既に暗号化されているコンテンツデータを復号する処理を行う。コーデック部25は、例えば、ATRAC（Adaptive Transform Acoustic Coding）3方式などでコンテンツデータをエンコードし、入出力インタフェース32を介してドライブ30に接続されている半導体メモリ44に供給し、記録させる。あるいは

また、コーデック部25は、ドライブ30を介して半導体メモリ44より読み出した、エンコードされているデータをデコードする。

【0027】半導体メモリ44は、例えば、メモリスティック（商標）などにより構成される。

【0028】CPU21、ROM22、RAM23、暗号化復号部24、およびコーデック部25は、バス31を介して相互に接続されている。このバス31にはまた、入出力インタフェース32も接続されている。

【0029】入出力インタフェース32には、キーボード、マウスなどよりなる入力部26、CRT、LCDなどよりなるディスプレイ、並びにスピーカなどよりなる出力部27、ハードディスクなどより構成される記憶部28、モデム、ターミナルアダプタなどより構成される通信部29が接続されている。通信部29は、インターネット2を介しての通信処理を行う。通信部29はまた、他のクライアントとの間で、アナログ信号またはデジタル信号の通信処理を行う。

【0030】入出力インタフェース32にはまた、必要に応じてドライブ30が接続され、磁気ディスク41、光ディスク42、光磁気ディスク43、或いは半導体メモリ44などが適宜装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部28にインストールされる。

【0031】なお、図示は省略するが、コンテンツサーバ3、ライセンスサーバ4、課金サーバ5も、図2に示したクライアント1と基本的に同様の構成を有するコンピュータにより構成される。そこで、以下の説明においては、図2の構成は、コンテンツサーバ3、ライセンスサーバ4、課金サーバ5などの構成としても引用される。

【0032】次に、図3のフローチャートを参照して、クライアント1がコンテンツサーバ3からコンテンツの提供を受ける処理について説明する。

【0033】ユーザが、入力部26を操作することでコンテンツサーバ3に対するアクセスを指令すると、CPU21は、ステップS1において、通信部29を制御し、インターネット2を介してコンテンツサーバ3にアクセスさせる。ステップS2において、ユーザが、入力部26を操作して、提供を受けるコンテンツを指定すると、CPU21は、この指定情報を受け取り、通信部29から、インターネット2を介してコンテンツサーバ3に、指定されたコンテンツを通知する。図4のフローチャートを参照して後述するように、この通知を受けたコンテンツサーバ3は、暗号化されたコンテンツデータを送信してくるので、ステップS3において、CPU21は、通信部29を介して、このコンテンツデータを受信すると、ステップS4において、その暗号化されているコンテンツデータを記憶部28を構成するハードディスクに供給し、記憶させる。

【0034】次に、図4のフローチャートを参照して、クライアント1の以上の処理に対応するコンテンツサーバ3のコンテンツ提供処理について説明する。なお、以下の説明において、図2のクライアント1の構成は、コンテンツサーバ3の構成としても引用される。

【0035】ステップS21において、コンテンツサーバ3のCPU21は、インターネット2から通信部29を介してクライアント1よりアクセスを受けるまで待機し、アクセスを受けたと判定したとき、ステップS22に進み、クライアント1から送信されてきたコンテンツを指定する情報を取り込む。このコンテンツを指定する情報は、クライアント1が、図3のステップS2において通知してきた情報である。

【0036】ステップS23において、コンテンツサーバ3のCPU21は、記憶部28に記憶されているコンテンツデータの中から、ステップS22の処理で取り込まれた情報で指定されたコンテンツを読み出す。CPU21は、ステップS24において、記憶部28から読み出されたコンテンツデータを、暗号化復号部24に供給し、コンテンツキーKcを用いて暗号化させる。

【0037】記憶部28に記憶されているコンテンツデータは、コーデック部25により、既にATRAC3方式によりエンコードされているので、このエンコードされているコンテンツデータが暗号化されることになる。

【0038】なお、もちろん、記憶部28に予め暗号化した状態でコンテンツデータを記憶させることができる。この場合には、ステップS24の処理は省略することが可能である。

【0039】次に、ステップS25において、コンテンツサーバ3のCPU21は、暗号化したコンテンツデータを伝送するフォーマットを構成するヘッダに、暗号化されているコンテンツを復号するのに必要なキー情報（図5を参照して後述するEKBと $K_{EKBc}$ （Kc））と、コンテンツを利用するのに必要なライセンスを識別するためのライセンスIDを付加する。そして、ステップS26において、コンテンツサーバ3のCPU21は、ステップS24の処理で暗号化したコンテンツと、ステップS25の処理でキーとライセンスIDを付加したヘッダとをフォーマット化したデータを、通信部29から、インターネット2を介して、アクセスしてきたクライアント1に送信する。

【0040】図5は、このようにして、コンテンツサーバ3からクライアント1にコンテンツが供給される場合のフォーマットの構成を表している。同図に示されるように、このフォーマットは、ヘッダ（Header）とデータ（Data）とにより構成される。

【0041】ヘッダには、コンテンツ情報（Content information）、デジタル権利管理情報（DRM（Digital Right Management） information）、ライセンスID（License ID）、イネープリングキーブロック（有効化キー

ブロック）（EKB（EnablingKey Block））および、EKBから生成されたキー $K_{EKBc}$ を用いて暗号化されたコンテンツキーKcとしてのデータ $K_{EKBc}$ （Kc）が配置されている。なお、EKBについては、図15を参照して後述する。

【0042】コンテンツ情報には、データとしてフォーマット化されているコンテンツデータを識別するための識別情報としてのコンテンツID（CID）、そのコンテンツのコーデックの方式などの情報が含まれている。

【0043】デジタル権利管理情報には、コンテンツを使用する規則および状態（Usage rules/status）と、URL（Uniform Resource Locator）が配置されている。使用規則および状態には、例えば、コンテンツの再生回数、コピー回数などが記述される。

【0044】URLは、ライセンスIDで規定されるライセンスを取得するときアクセスするアドレス情報であり、図1のシステムの場合、具体的には、ライセンスを受けるために必要なライセンスサーバ4のアドレスである。ライセンスIDは、データとして記録されているコンテンツを利用するとき必要とされるライセンスを識別するものである。

【0045】データは、任意の数の暗号化ブロック（Encryption Block）により構成される。各暗号化ブロックは、イニシャルベクトル（IV（Initial Vector））、シード（Seed）、およびコンテンツデータをキー $K'c$ で暗号化したデータ $Ex'c$ （data）により構成されている。

【0046】キー $K'c$ は、次式により示されるように、コンテンツキーKcと、乱数で設定される値Seedをハッシュ関数に適用して演算された値により構成される。

【0047】 $K'c = \text{Hash}(Kc, \text{Seed})$

【0048】イニシャルベクトルIVとシードSeedは、各暗号化ブロック毎に異なる値に設定される。

【0049】この暗号化は、コンテンツのデータを8バイト単位で区分して、8バイト毎に行われる。後段の8バイトの暗号化は、前段の8バイトの暗号化の結果を利用して行われるCBC（Cipher Block Chaining）モードで行われる。

【0050】CBCモードの場合、最初の8バイトのコンテンツデータを暗号化するとき、その前段の8バイトの暗号化結果が存在しないため、最初の8バイトのコンテンツデータを暗号化するときは、イニシャルベクトルIVを初期値として暗号化が行われる。

【0051】このCBCモードによる暗号化を行うことで、1つの暗号化ブロックが解読されたとしても、その影響が、他の暗号化ブロックにおよぶことが抑制される。

【0052】なお、この暗号化については、図46を参照にして、後に詳述する。

【0053】また、暗号方式についてはこれに限らない。

【0054】以上のようにして、クライアント1は、コンテンツサーバ3からコンテンツを無料で、自由に取得することができる。従って、コンテンツそのものは、大量に、配布することが可能となる。

【0055】しかしながら、各クライアント1は、取得したコンテンツを利用するとき、ライセンスを保持している必要がある。そこで、図6を参照して、クライアント1がコンテンツを再生する場合の処理について説明する。

【0056】ステップS41において、クライアント1のCPU21は、ユーザが入力部26を操作することで指示したコンテンツの識別情報(CID)を取得する。この識別情報は、例えば、コンテンツのタイトルや、記憶されている各コンテンツ毎に付与されている番号などにより構成される。

【0057】そして、CPU21は、コンテンツが指示されると、そのコンテンツに対応するライセンスID(そのコンテンツを使用するのに必要なライセンスのID)を読み取る。このライセンスIDは、図5に示されるように、暗号化されているコンテンツデータのヘッダに記述されているものである。

【0058】次に、ステップS42に進み、CPU21は、ステップS41で読み取られたライセンスIDに対応するライセンスが、クライアント1により既に取得され、記憶部28に記憶されているか否かを判定する。まだ、ライセンスが取得されていない場合には、ステップS43に進み、CPU21は、ライセンス取得処理を実行する。このライセンス取得処理の詳細は、図7のフローチャートを参照して後述する。

【0059】ステップS42において、ライセンスが既に取得されていると判定された場合、または、ステップS43において、ライセンス取得処理が実行された結果、ライセンスが取得された場合、ステップS44に進み、CPU21は、取得されているライセンスは有効期限内のものであるか否かを判定する。ライセンスが有効期限内のものであるか否かは、ライセンスの内容として規定されている期限(後述する図8参照)と、タイマ20により計時されている現在日時と比較することで判断される。ライセンスの有効期限が既に満了していると判定された場合、CPU21は、ステップS45に進み、ライセンス更新処理を実行する。このライセンス更新処理の詳細は、図10のフローチャートを参照して後述する。

【0060】ステップS44において、ライセンスはまだ有効期限内であると判定された場合、または、ステップS45において、ライセンスが更新された場合、ステップS46に進み、CPU21は、暗号化されているコンテンツデータを記憶部28から読み出し、RAM23に格納させる。そして、ステップS47において、CPU21は、RAM23に記憶された暗号化ブロックのデータを、図5のデータに配置されている暗号化ブロック単位で、

暗号化復号部24に供給し、コンテンツキーKcを用いて復号させる。

【0061】コンテンツキーKcを得る方法の具体例は、図15を参照して後述するが、デバイスノードキー(DNK)(図8)を用いて、EKB(図5)に含まれるキーK<sub>EKBC</sub>を得ることができ、そのキーK<sub>EKBC</sub>を用いて、データK<sub>EKBC</sub>(Kc)(図5)から、コンテンツキーKcを得ることができる。

【0062】CPU21は、さらに、ステップS48において、暗号化復号部24により復号されたコンテンツデータをコーデック部25に供給し、デコードさせる。そして、コーデック部25によりデコードされたデータを、CPU21は、入出力インタフェース32から出力部27に供給し、D/A変換させ、スピーカから出力させる。

【0063】次に、図7のフローチャートを参照して、図6のステップS43で行われるライセンス取得処理の詳細について説明する。

【0064】クライアント1は、事前にライセンスサーバに登録することにより、リーフID、DNK(Device Node Key)、クライアント1の秘密鍵・公開鍵のペア、ライセンスサーバの公開鍵、及び各公開鍵の証明書を含むサービスデータを取得しておく。

【0065】リーフIDは、クライアント毎に割り当てられた識別情報を表し、DNKは、そのライセンスに対応するEKB(有効化キーブロック)に含まれる暗号化されているコンテンツキーKcを復号するのに必要なデバイスノードキーである(図12を参照して後述する)。

【0066】最初にステップS61において、CPU21は、いま処理対象とされているライセンスIDに対応するURLを、図5に示すヘッダから取得する。上述したように、このURLは、やはりヘッダに記述されているライセンスIDに対応するライセンスを取得するときアクセスすべきアドレスである。そこで、ステップS62において、CPU21は、ステップS61で取得したURLにアクセスする。具体的には、通信部29によりインターネット2を介してライセンスサーバ4にアクセスが行われる。このとき、ライセンスサーバ4は、クライアント1に対して、購入するライセンス(コンテンツを使用するのに必要なライセンス)を指定するライセンス指定情報、並びにユーザIDとパスワードの入力を要求してくる(後述する図9のステップS102)。CPU21は、この要求を出力部27の表示部に表示させる。ユーザは、この表示に基づいて、入力部26を操作して、ライセンス指定情報、ユーザID、およびパスワードを入力する。なお、このユーザIDとパスワードは、クライアント1のユーザが、インターネット2を介してライセンスサーバ4にアクセスし、事前に取得しておいたものである。

【0067】CPU21は、ステップS63、S64において、入力部26から入力されたライセンス識別情報を

取り込むとともに、ユーザIDとパスワードを取り込む。CPU 2 1は、ステップS 6 5において、通信部2 9を制御し、入力されたユーザIDとパスワードを、ライセンス指定情報及びサービスデータ（後述する）に含まれるリーフIDを含むライセンス要求をインターネット2を介してライセンスサーバ4に送信させる。

【0068】ライセンスサーバ4は、図9を参照して後述するように、ユーザIDとパスワード、並びにライセンス指定情報に基づいてライセンスを送信してくる（ステップS 1 0 9）か、または、条件が満たされない場合には、ライセンスを送信してこない（ステップS 1 1 2）。

【0069】ステップS 6 6において、CPU 2 1は、ライセンスサーバ4からライセンスが送信されてきたか否かを判定し、ライセンスが送信されてきた場合には、ステップS 6 7に進み、そのライセンスを記憶部2 8に供給し、記憶させる。

【0070】ステップS 6 6において、ライセンスが送信されて来ないと判定した場合、CPU 2 1は、ステップS 6 8に進み、エラー処理を実行する。具体的には、CPU 2 1は、コンテンツを利用するためのライセンスが得られないので、コンテンツの再生処理を禁止する。

【0071】以上のようにして、各クライアント1は、コンテンツデータに付随しているライセンスIDに対応するライセンスを取得して、初めて、そのコンテンツを使用することが可能となる。

【0072】なお、図7のライセンス取得処理は、各ユーザがコンテンツを取得する前に、予め行っておくようにすることも可能である。

【0073】クライアント1に提供されるライセンスは、例えば、図8に示されるように、使用条件、リーフIDおよびを含んでいる。

【0074】使用条件には、そのライセンスに基づいて、コンテンツを使用することが可能な使用期限、そのライセンスに基づいて、コンテンツをダウンロードすることが可能なダウンロード期限、そのライセンスに基づいて、コンテンツをコピーすることが可能な回数（許されるコピー回数）、チェックアウト回数、最大チェックアウト回数、そのライセンスに基づいて、コンテンツをCD-Rに記録することができる権利、PD（Portable Device）にコピーすることが可能な回数、ライセンスを所有権（買い取り状態）に移行できる権利、使用ログをとる義務等を示す情報が含まれる。

【0075】次に、図9のフローチャートを参照して、図7のクライアント1のライセンス取得処理に対応して実行されるライセンスサーバ4のライセンス提供処理について説明する。なお、この場合においても、図2のクライアント1の構成は、ライセンスサーバ4の構成として引用される。

【0076】ステップS 1 0 1において、ライセンスサ

サーバ4のCPU 2 1は、クライアント1よりアクセスを受けるまで待機し、アクセスを受けたとき、ステップS 1 0 2に進み、アクセスしてきたクライアント1に対して、ユーザIDとパスワード、並びに、ライセンス指定情報の送信を要求する。上述したようにして、クライアント1から、図7のステップS 6 5の処理で、ユーザIDとパスワード、リーフID並びにライセンス指定情報（ライセンスID）が送信されてきたとき、ライセンスサーバ4のCPU 2 1は、通信部2 9を介してこれを受信し、取り込む処理を実行する。

【0077】そして、ライセンスサーバ4のCPU 2 1は、ステップS 1 0 3において、通信部2 9から課金サーバ5にアクセスし、ユーザIDとパスワードに対応するユーザの与信処理を要求する。課金サーバ5は、インターネット2を介してライセンスサーバ4から与信処理の要求を受けると、そのユーザIDとパスワードに対応するユーザの過去の支払い履歴などを調査し、そのユーザが、過去にライセンスの対価の不払いの実績があるか否かなどを調べ、そのような実績がない場合には、ライセンスの付与を許容する与信結果を送信し、不払いの実績などがある場合には、ライセンス付与の不許可の与信結果を送信する。

【0078】ステップS 1 0 4において、ライセンスサーバ4のCPU 2 1は、課金サーバ5からの与信結果が、ライセンスを付与することを許容する与信結果であるか否かを判定し、ライセンスの付与が許容されている場合には、ステップS 1 0 5に進み、ステップS 1 0 2の処理で取り込まれたライセンス指定情報に対応するライセンスを、記憶部2 8に記憶されているライセンスの中から取り出す。記憶部2 8に記憶されているライセンスは、あらかじめライセンスID、バージョン、作成日時、有効期限等の情報が記述されている。ステップS 1 0 6において、CPU 2 1は、そのライセンスに受信したリーフIDを付加する。さらに、ステップS 1 0 7において、CPU 2 1は、ステップS 1 0 5で選択されたライセンスに対応づけられている使用条件を選択する。あるいはまた、ステップS 1 0 2の処理で、ユーザから使用条件が指定された場合には、その使用条件が必要に応じて、予め用意されている使用条件に付加される。CPU 2 1は、選択された使用条件をライセンスに付加する。

【0079】ステップS 1 0 8において、CPU 2 1はライセンスサーバの秘密鍵によりライセンスに署名し、これにより、図8に示されるような構成のライセンスが生成される。

【0080】次に、ステップS 1 0 9に進み、ライセンスサーバ4のCPU 2 1は、そのライセンス（図8に示される構成を有する）を、通信部2 9からインターネット2を介してクライアント1に送信させる。

【0081】ステップS 1 1 0においてライセンスサーバ4のCPU 2 1は、ステップS 1 0 9の処理で、いま送

信したライセンス（使用条件、リーフIDを含む）を、ステップS102の処理で取り込まれたユーザIDとパスワードに対応して、記憶部28に記憶させる。さらに、ステップS111において、CPU21は、課金処理を実行する。具体的には、CPU21は、通信部29から課金サーバ5に、そのユーザIDとパスワードに対応するユーザに対する課金処理を要求する。課金サーバ5は、この課金の要求に基づいて、そのユーザに対する課金処理を実行する。上述したように、この課金処理に対して、そのユーザが支払いを行わなかったような場合には、以後、そのユーザは、ライセンスの付与を要求したとしても、ライセンスを受けることができないことになる。

【0082】すなわち、この場合には、課金サーバ5からライセンスの付与を不許可とする受信結果が送信されてくるので、ステップS104からステップS112に進み、CPU21は、エラー処理を実行する。具体的には、ライセンスサーバ4のCPU21は、通信部29を制御してアクセスしてきたクライアント1に対して、ライセンスを付与することができない旨のメッセージを出力し、処理を終了させる。

【0083】この場合、上述したように、そのクライアント1はライセンスを受けることができないので、そのコンテンツを利用すること（暗号を復号すること）ができないことになる。

【0084】図10は、図6のステップS45におけるライセンス更新処理の詳細を表している。図10のステップS131乃至ステップS135の処理は、図7のステップS61乃至ステップS65の処理と基本的に同様の処理である。ただし、ステップS133において、CPU21は、購入するライセンスではなく、更新するライセンスのライセンスIDを取り込む。そして、ステップS135において、CPU21は、ユーザIDとパスワードとともに、更新するライセンスのライセンスIDを、ライセンスサーバ4に送信する。

【0085】ステップS135の送信処理に対応して、ライセンスサーバ4は、後述するように、使用条件を提示してくる（図11のステップS153）。そこで、クライアント1のCPU21は、ステップS136において、ライセンスサーバ4からの使用条件の提示を受信し、これを出力部27に出力し、表示させる。ユーザは、入力部26を操作して、この使用条件の中から所定の使用条件を選択したり、所定の使用条件を新たに追加したりする。ステップS137でCPU21は、以上のようにして選択された使用条件（ライセンスを更新する条件）を購入するための申し込みをライセンスサーバ4に送信する。この申し込みに対応して、後述するようにライセンスサーバ4は、最終的な使用条件を送信してくる（図11のステップS154）。そこで、ステップS138において、クライアント1のCPU21は、ライセンスサーバ4からの使用条件を取得し、ステップS139

において、その使用条件を記憶部28にすでに記憶されている対応するライセンスの使用条件として更新する。

【0086】図11は、以上のクライアント1のライセンス更新処理に対応して、ライセンスサーバ4が実行するライセンス更新処理を表している。

【0087】最初に、ステップS151において、ライセンスサーバ4のCPU21は、クライアント1からのアクセスを受けると、ステップS152において、クライアント1がステップS135で送信したライセンス指定情報をライセンス更新要求情報とともに受信する。

【0088】ステップS153において、CPU21は、ライセンスの更新要求を受信すると、そのライセンスに対応する使用条件（更新する使用条件）を、記憶部28から読み出し、クライアント1に送信する。

【0089】この提示に対して、上述したように、クライアント1から使用条件の購入が図10のステップS137の処理で申し込まれると、ステップS154において、ライセンスサーバ4のCPU21は、申し込まれた使用条件に対応するデータを生成し、ステップS154において、クライアント1に送信する。クライアント1は、上述したように、ステップS139の処理で受信した使用条件を用いて、すでに登録されているライセンスの使用条件を更新する。

【0090】本発明においては、図12に示されるように、ブロードキャストインクリプション（Broadcast Encryption）方式の原理に基づいて、デバイスとライセンスのキーが管理される。キーは、階層ツリー構造とされ、最下段のリーフ（leaf）が個々のデバイスのキーに対応する。図12の例の場合、番号0から番号15までの16個のデバイスまたはライセンスに対応するキーが生成される。

【0091】各キーは、図中丸印で示されるツリー構造の各ノードに対応して規定される。この例では、最上段のルートノードに対応してルートキーKRが、2段目のノードに対応してキーK0、K1が、3段目のノードに対応してキーK00乃至K11が、第4段目のノードに対応してキーK000乃至キーK111が、それぞれ対応されている。そして、最下段のノードとしてのリーフ（デバイスノード）に、キーK0000乃至K1111が、それぞれ対応されている。

【0092】階層構造とされているため、例えば、キーK0010とキー0011の上位のキーは、K001とされ、キーK000とキーK001の上位のキーは、K00とされている。以下同様に、キーK00とキーK01の上位のキーは、K0とされ、キーK0とキーK1の上位のキーは、KRとされている。

【0093】コンテンツを利用するキーは、最下段のデバイスノード（リーフ）から、最上段のルートノードまでの1つのパスの各ノードに対応するキーで管理される。例えば、番号3のノード（リーフID）に対応するラ

イセンスに基づき、コンテンツを利用するキーは、キーK0011, K001, K00, K0, KRを含むパスの各キーで管理される。

【0094】本発明のシステムにおいては、図13に示されるように、図12の原理に基づいて構成されるキーシステムで、デバイスのキーとライセンスのキーの管理が行われる。図13の例では、8+24+32段のノードがツリー構造とされ、ルートノードから下位の8段までの各ノードにカテゴリが対応される。ここにおけるカテゴリとは、例えばメモリスティックなどの半導体メモリを使用する機器のカテゴリ、デジタル放送を受信する機器のカテゴリといったカテゴリを意味する。そして、このカテゴリノードのうちの1つのノードに、ライセンスを管理するシステムとして本システム（Tシステムと称する）が対応する。

【0095】すなわち、このTシステムのノードよりさらに下の階層の24段のノードに対応するキーにより、ライセンスが対応される。この例の場合、これにより、 $2^{24}$ （約16メガ）のライセンスを規定することができる。さらに、最も下側の32段の階層により、 $2^{32}$ （約4ギガ）のユーザ（あるいはクライアント1）を規定することができる。最下段の32段のノードに対応するキーが、DNK（Device Node Key）を構成し、最下段のリーフに対応するIDがリーフIDとされる。

【0096】各デバイスやライセンスのキーは、64（=8+24+32）段の各ノードで構成されるパスの内の1つに対応される。例えば、コンテンツを暗号化したコンテンツキーは、対応するライセンスに割り当てられたパスを構成するノードに対応するキーを用いて暗号化される。上位の階層のキーは、その直近の下位の階層のキーを用いて暗号化され、EKB（図15を参照して後述する）内に配置される。最下段のDNKは、EKB内には配置されず、サービスデータに記述され、ユーザのクライアント1に与えられる。クライアント1は、ライセンスに記述されているDNKを用いて、コンテンツデータとともに配布されるEKB（図15）内に記述されている直近の上位の階層のキーを復号し、復号して得たキーを用いて、EKB内に記述されているさらにその上の階層のキーを復号する。以上の処理を順次行うことで、クライアント1は、そのライセンスのパスに属するすべてのキーを得ることができる。

【0097】図14に階層ツリー構造のカテゴリの分類の具体的な例を示す。図14において、階層ツリー構造の最上段には、ルートキーKR2301が設定され、以下の中間段にはノードキー2302が設定され、最下段には、リーフキー2303が設定される。各デバイスは個々のリーフキーと、リーフキーからルートキーに至る一連のノードキー、ルートキーを保有する。

【0098】最上段から第M段目（図13の例では、M=8）の所定のノードがカテゴリノード2304として

設定される。すなわち第M段目のノードの各々が特定カテゴリのデバイス設定ノードとされる。第M段の1つのノードを頂点としてM+1段以下のノード、リーフは、そのカテゴリに含まれるデバイスに関するノードおよびリーフとされる。

【0099】例えば図14の第M段目の1つのノード2305にはカテゴリ「メモリスティック（商標）」が設定され、このノード以下に連なるノード、リーフはメモリスティックを使用した様々なデバイスを含むカテゴリ専用のノードまたはリーフとして設定される。すなわち、ノード2305以下が、メモリスティックのカテゴリに定義されるデバイスの関連ノード、およびリーフの集合として定義される。

【0100】さらに、M段から数段分下位の段をサブカテゴリノード2306として設定することができる。図14の例では、カテゴリ「メモリスティック」ノード2305の2段下のノードに、メモリスティックを使用したデバイスのカテゴリに含まれるサブカテゴリノードとして、「再生専用器」のノード2306が設定されている。さらに、サブカテゴリノードである再生専用器のノード2306以下に、再生専用器のカテゴリに含まれる音楽再生機能付き電話のノード2307が設定され、さらにその下位に、音楽再生機能付き電話のカテゴリに含まれる「PHS」ノード2308と、「携帯電話」ノード2309が設定されている。

【0101】さらに、カテゴリ、サブカテゴリは、デバイスの種類のみならず、例えばあるメーカー、コンテンツプロバイダ、決済機関等が独自に管理するノード、すなわち処理単位、管轄単位、あるいは提供サービス単位等、任意の単位（これらを総称して以下、エンティティと呼ぶ）で設定することが可能である。例えば1つのカテゴリノードをゲーム機器メーカーの販売するゲーム機器XYZ専用の頂点ノードとして設定すれば、メーカーの販売するゲーム機器XYZに、その頂点ノード以下の下段のノードキー、リーフキーを格納して販売することが可能となり、その後、暗号化コンテンツの配信、あるいは各種キーの配信、更新処理を、その頂点ノードキー以下のノードキー、リーフキーによって構成される有効化キーブロック（EKB）を生成して配信し、頂点ノード以下のデバイスに対してのみ利用可能なデータが配信可能となる。

【0102】このように、1つのノードを頂点として、以下のノードをその頂点ノードに定義されたカテゴリ、あるいはサブカテゴリの関連ノードとして設定する構成とすることにより、カテゴリ段、あるいはサブカテゴリ段の1つの頂点ノードを管理するメーカー、コンテンツプロバイダ等がそのノードを頂点とする有効化キーブロック（EKB）を独自に生成して、頂点ノード以下に属するデバイスに配信する構成が可能となり、頂点ノードに属さない他のカテゴリのノードに属するデバイスには

全く影響を及ぼさずにキー更新を実行することができる。

【0103】例えば、図12に示されるツリー構造において、1つのグループに含まれる4つのデバイス0、1、2、3はノードキーとして共通のキーK00、K0、KRを保有する。このノードキー共有構成を利用することにより、共通のコンテンツキーをデバイス0、1、2、3のみに提供することが可能となる。たとえば、共通に保有するノードキーK00自体をコンテンツキーとして設定すれば、新たな鍵送付を実行することなくデバイス0、1、2、3のみが共通のコンテンツキーの設定が可能である。また、新たなコンテンツキーKconをノードキーK00で暗号化した値Enc(K00, Kcon)を、ネットワークを介してあるいは記録媒体に格納してデバイス0、1、2、3に配布すれば、デバイス0、1、2、3のみが、それぞれのデバイスにおいて保有する共有ノードキーK00を用いて暗号Enc(K00, Kcon)を解いてコンテンツキーKconを得ることが可能となる。なお、Enc(Ka, Kb)はKbをKaによって暗号化したデータであることを示す。

【0104】また、ある時点tにおいて、デバイス3の所有する鍵K0011, K001, K00, K0, KRが攻撃者(ハッカー)により解析されて露呈したことが発覚した場合、それ以降、システム(デバイス0、1、2、3のグループ)で送受信されるデータを守るために、デバイス3をシステムから切り離す必要がある。そのためには、ノードキーK001, K00, K0, KRを、それぞれ新たな鍵K(t)001, K(t)00, K(t)0, K(t)Rに更新し、デバイス0、1、2にその更新キーを伝える必要がある。ここで、K(t)aaaは、鍵Kaaaの世代(Generation)tの更新キーであることを示す。

【0105】更新キーの配布処理について説明する。キーの更新は、例えば、図15Aに示す有効化キーブロック(EKB: Enabling Key Block)と呼ばれるブロックデータによって構成されるテーブルを、ネットワークを介して、あるいは記録媒体に格納してデバイス0、1、2に供給することによって実行される。なお、有効化キーブロック(EKB)は、図12に示されるようなツリー構造を構成する各リーフ(最下段のノード)に対応するデバイスに、新たに更新されたキーを配布するための暗号化キーによって構成される。有効化キーブロック(EKB)は、キー更新ブロック(KRB: Key Renewal Block)と呼ばれることもある。

【0106】図15Aに示す有効化キーブロック(EKB)は、ノードキーの更新に必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図15Aの例は、図12に示すツリー構造中のデバイス0、1、2において、世代tの更新ノードキーを配布することを目的として形成されたブロックデータであ

る。図12から明らかなように、デバイス0、デバイス1は、更新ノードキーとしてK(t)00、K(t)0、K(t)Rが必要であり、デバイス2は、更新ノードキーとしてK(t)001、K(t)00、K(t)0、K(t)Rが必要である。

【0107】図15AのEKBに示されるように、EKBには複数の暗号化キーが含まれる。図15Aの最下段の暗号化キーは、Enc(K0010, K(t)001)である。これはデバイス2の持つリーフキーK0010によって暗号化された更新ノードキーK(t)001であり、デバイス2は、自身の持つリーフキーK0010によってこの暗号化キーを復号し、更新ノードキーK(t)001を得ることができる。また、復号により得た更新ノードキーK(t)001を用いて、図15Aの下から2段目の暗号化キーEnc(K(t)001, K(t)00)が復号可能となり、更新ノードキーK(t)00を得ることができる。

【0108】以下順次、図15Aの上から2段目の暗号化キーEnc(K(t)00, K(t)0)を復号することで、更新ノードキーK(t)0が得られ、これを用いて、図15Aの上から1段目の暗号化キーEnc(K(t)0, K(t)R)を復号することで、更新ルートキーK(t)Rが得られる。

【0109】一方、ノードキーK000は更新する対象に含まれておらず、ノード0、1が、更新ノードキーとして必要なのは、K(t)00、K(t)0、K(t)Rである。ノード0、1は、デバイスキーK0000、K0001を用いて、図15Aの上から3段目の暗号化キーEnc(K000, K(t)00)を復号することで更新ノードキーK(t)00を取得し、以下順次、図15Aの上から2段目の暗号化キーEnc(K(t)00, K(t)0)を復号することで、更新ノードキーK(t)0を得、図15Aの上から1段目の暗号化キーEnc(K(t)0, K(t)R)を復号することで、更新ルートキーK(t)Rを得る。このようにして、デバイス0、1、2は更新したキーK(t)Rを得ることができる。

【0110】なお、図15Aのインデックスは、図の右側の暗号化キーを復号するための復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

【0111】図12に示すツリー構造の上位段のノードキーK(t)0、K(t)Rの更新が不要であり、ノードキーK00のみの更新処理が必要である場合には、図15Bの有効化キーブロック(EKB)を用いることで、更新ノードキーK(t)00をデバイス0、1、2に配布することができる。

【0112】図15Bに示すEKBは、例えば特定のグループにおいて共有する新たなコンテンツキーを配布する場合に利用可能である。具体例として、図12に点線で示すグループ内のデバイス0、1、2、3がある記録

媒体を用いており、新たな共通のコンテンツキー  $K(t)con$  が必要であるとする。このとき、デバイス 0, 1, 2, 3 の共通のノードキー  $K00$  を更新した  $K(t)00$  を用いて新たな共通の更新コンテンツキー  $K(t)con$  を暗号化したデータ  $Enc(K(t)00, K(t)con)$  が、図 15 B に示される  $EKB$  とともに配布される。この配布により、デバイス 4 など、その他のグループの機器が復号することができないデータとしての配布が可能となる。

【0113】すなわち、デバイス 0, 1, 2 は  $EKB$  を処理して得たキー  $K(t)00$  を用いて暗号文を復号すれば、 $t$  時点でのコンテンツキー  $K(t)con$  を得ることが可能になる。

【0114】図 16 に、 $t$  時点でのコンテンツキー  $K(t)con$  を得る処理例として、 $K(t)00$  を用いて新たな共通のコンテンツキー  $K(t)con$  を暗号化したデータ  $Enc(K(t)00, K(t)con)$  と、図 15 B に示す  $EKB$  とを記録媒体を介して受領したデバイス 0 の処理を示す。すなわちこの例は、 $EKB$  による暗号化メッセージデータをコンテンツキー  $K(t)con$  とした例である。

【0115】図 16 に示すように、デバイス 0 は、記録媒体に格納されている世代  $t$  時点の  $EKB$  と、自分があらかじめ格納しているノードキー  $K000$  を用いて、上述したと同様の  $EKB$  処理により、ノードキー  $K(t)00$  を生成する。さらに、デバイス 0 は、復号した更新ノードキー  $K(t)00$  を用いて、更新コンテンツキー  $K(t)con$  を復号して、後にそれを使用するために自分だけが持つリーフキー  $K0000$  で暗号化して格納する。

【0116】図 17 に有効化キープロック ( $EKB$ ) のフォーマット例を示す。バージョン 601 は、有効化キープロック ( $EKB$ ) のバージョンを示す識別子である。なお、バージョンは、最新の  $EKB$  を識別する機能と、コンテンツとの対応関係を示す機能を持つ。デプスは、有効化キープロック ( $EKB$ ) の配布先のデバイスに対する階層ツリーの階層数を示す。データポイント 603 は、有効化キープロック ( $EKB$ ) 中のデータ部 606 の位置を示すポイントであり、タグポイント 604 はタグ部 607 の位置、署名ポイント 605 は署名 608 の位置を示すポイントである。

【0117】データ部 606 は、例えば更新するノードキーを暗号化したデータを格納する。例えば図 16 に示すような更新されたノードキーに関する各暗号化キー等を格納する。

【0118】タグ部 607 は、データ部 606 に格納された暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールを図 18 を用いて説明する。

【0119】図 18 では、データとして先に図 15 A で

説明した有効化キープロック ( $EKB$ ) を送付する例を示している。この時のデータは、図 18 B の表に示ようになる。このときの暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。この例の場合は、ルートキーの更新キー  $K(t)R$  が含まれているので、トップノードアドレスは  $KR$  となる。このとき、例えば最上段のデータ  $Enc(K(t)0, K(t)R)$  は、図 18 A に示す階層ツリーに示す位置  $P0$  に対応する。次の段のデータは、 $Enc(K(t)00, K(t)0)$  であり、ツリー上では前のデータの左下の位置  $P00$  に対応する。ツリー構造の所定の位置から見て、その下に、データがある場合は、タグが 0、ない場合はタグが 1 に設定される。タグは {左 (L) タグ, 右 (R) タグ} として設定される。図 18 B の最上段のデータ  $Enc(K(t)0, K(t)R)$  に対応する位置  $P0$  の左下の位置  $P00$  にはデータがあるので、L タグ = 0、右にはデータがないので、R タグ = 1 となる。以下、すべてのデータにタグが設定され、図 18 C に示すデータ列、およびタグ列が構成される。

【0120】タグは、対応するデータ  $Enc(Kxx, Kyyy)$  が、ツリー構造のどこに位置しているのかを示すために設定されるものである。データ部 606 に格納されるキーデータ  $Enc(Kxxx, Kyyy) \dots$  は、単純に暗号化されたキーの羅列データに過ぎないが、上述したタグによってデータとして格納された暗号化キーのツリー上の位置が判別可能となる。上述したタグを用いずに、先の図 15 で説明した構成のように、暗号化データに対応させたノード・インデックスを用いて、例えば、

0 :  $Enc(K(t)0, K(t)R)$   
 00 :  $Enc(K(t)00, K(t)0)$   
 000 :  $Enc(K(t)000, K(t)00)$   
 ... のようなデータ構成とすることも可能であるが、このようなインデックスを用いた構成とすると、冗長なデータとなりデータ量が増大し、ネットワークを介する配信等においては好ましくない。これに対し、上述したタグをキー位置を示す索引データとして用いることにより、少ないデータ量でキー位置の判別が可能となる。

【0121】図 17 に戻って、 $EKB$  フォーマットについてさらに説明する。署名 (Signature) 608 は、有効化キープロック ( $EKB$ ) を発行した例えば鍵管理センタ (ライセンスサーバ 4)、コンテンツロバイダ (コンテンツサーバ 3)、決済機関 (課金サーバ 5) 等が実行する電子署名である。 $EKB$  を受領したデバイスは、署名検証によって正当な有効化キープロック ( $EKB$ ) 発行者が発行した有効化キープロック ( $EKB$ ) であることを確認する。

【0122】以上のようにして、ライセンスサーバ 4 から供給されたライセンスに基づいて、コンテンツサーバ 3 から供給されたコンテンツを利用する処理をまとめる

と、図19に示されるようになる。

【0123】すなわち、コンテンツサーバ3からクライアント1に対してコンテンツが提供されるとともに、ライセンスサーバ4からクライアント1にライセンスが供給される。コンテンツは、コンテンツキーKcにより、暗号化されており(Enc(Kc, Content))、コンテンツキーKcは、ルートキーKR(EKBから得られるキーであって、図5におけるキーK<sub>EKB</sub>に対応する)で暗号化され(Enc(KR, Kc))、EKBとともに、暗号化されたコンテンツに付加されてクライアント1に提供される。

【0124】図19の例におけるEKBには、例えば、図20に示されるように、DNKで暗号化したルートキーKRが含まれている(Enc(DNK, KR))。従って、クライアント1は、サービスデータに含まれるDNKを利用して、EKBからルートキーKRを得ることができる。さらに、ルートキーKRを用いて、Enc(KR, Kc)からコンテンツキーKcを復号することができ、コンテンツキーKcを用いて、Enc(Kc, Content)からコンテンツを復号することができる。

【0125】このように、クライアント1にDNKを個別に割り当てることにより、図12と図15を参照して説明した原理に従って、個々のクライアント1のリボーク(revoke)が可能になる。

【0126】また、ライセンスリーフIDを付加して配布することにより、クライアント1において、サービスデータとライセンスの対応付けが行われることになり、ライセンスの不正コピーを防止することが可能になる。

【0127】また、クライアント用の証明書と秘密鍵をサービスデータとして配信するようにすることで、エンドユーザも、これらを用いて不正コピーを防止可能なコンテンツを作成することが可能になる。

【0128】証明書と秘密鍵の利用については、図28のフローチャートを参照して後述する。

【0129】本発明においては、図13を参照して説明したように、カテゴリノードにライセンスを管理するTシステムと、各種のコンテンツを利用するデバイスのカテゴリが対応づけられるので、複数のDNKを同一のデバイスに持たせることができる。その結果、異なるカテゴリのコンテンツを1つのデバイスで管理することが可能となる。

【0130】図21は、この関係を表している。すなわち、デバイスD1には、Tシステムに基づいて、DNK1が割り当てられている、コンテンツ1を利用するライセンスが記録される。同様に、このデバイスD1には、例えば、DNK2が割り当てられた、メモリスティックにCDからリッピングしたコンテンツ2を記録することができる。この場合、デバイスD1は、コンテンツ1とコンテンツ2という、異なるシステム(Tシステムとデバイス管理システム)により配信されたコンテンツを同時に扱うことが可能となる。新たなDNKを割り当てるとき、既

に割り当てられているDNKを削除するなどして、デバイスに1個のDNKだけを対応させるようにした場合、このようなことはできない。

【0131】また、図13における、例えば、下側の32階層の各三角形の1つ1つに、図22に示されるライセンスカテゴリ1とライセンスカテゴリ2を割り当てることにより、同一のカテゴリ内を、サブカテゴリを利用して、コンテンツのジャンル、レーベル、販売店、配信サービス等の小さな集まりに分類して、管理することが可能となる。

【0132】図22の例においては、例えば、ライセンスカテゴリ1は、ジャズのジャンルに属し、ライセンスカテゴリ2は、ロックのジャンルに属する。ライセンスカテゴリ1には、ライセンスIDが1であるコンテンツ1とコンテンツ2を対応させ、それぞれユーザ1乃至ユーザ3に配布されている。ライセンスカテゴリ2は、ライセンスID2のコンテンツ3、コンテンツ4、およびコンテンツ5が含まれ、それぞれユーザ1とユーザ3に提供されている。

【0133】このように、本発明においては、カテゴリ毎に独立したキー管理が可能になる。

【0134】また、DNKを、機器やメディアに予め埋め込むのではなく、ライセンスサーバ4により、登録処理を行う際に、各機器やメディアにダウンロードするようにすることで、ユーザによるキーの購入が可能なシステムを実現することができる。

【0135】コンテンツは、それが作成された後、どのような使われ方をされようとも、その使われ方に関わりなく、全ての用途において、使用可能であるのが望ましい。例えば、異なるコンテンツ配信サービス、あるいは使用条件が異なるドメインにおいても、同一のコンテンツが使えることが望ましい。本発明においては、このため、上述したように、各ユーザ(クライアント1)に、認証局としてのライセンスサーバ4から秘密鍵と、それに対応する公開鍵の証明書(certificates)が配布される。各ユーザは、その秘密鍵を用いて、署名(signature)を作成し、コンテンツに付加して、コンテンツの真正さ(integrity)を保証し、かつコンテンツの改竄防止を図ることができる。

【0136】この場合の処理の例について、図23のフローチャートを参照して説明する。図23の処理は、ユーザがCDから再生したデータを記憶部28に記憶させるリッピング処理を説明するものである。

【0137】最初に、ステップS171において、クライアント1のCPU21は、通信部29を介して入力されるCDの再生データを記録データとして取り込む。ステップS172において、CPU21は、ステップS171の処理で取り込まれた記録データにウォーターマークが含まれているか否かを判定する。このウォーターマークは、3ビットのコピー管理情報(CCI)と、1ビットの

トリガ (Trigger) とにより構成され、コンテンツのデータの中に埋め込まれている。CPU 21は、ウォーターマークが検出された場合には、ステップ S 173に進み、そのウォーターマークを抽出する処理を実行する。ウォーターマークが存在しない場合には、ステップ S 173の処理はスキップされる。

【0138】次に、ステップ S 174において、CPU 21は、コンテンツに対応して記録するヘッダのデータを作成する。このヘッダのデータは、コンテンツID、ライセンスID、ライセンスを取得するためのアクセス先を表すURL、およびウォーターマークにより構成される。

【0139】次に、ステップ S 175に進み、CPU 21は、ステップ S 174の処理で作成したヘッダのデータに基づいたデジタル署名を、自分自身の秘密鍵を用いて作成する。この秘密鍵は、ライセンスサーバ4から取得したものである (図7のステップ S 67)。

【0140】ステップ S 176で、CPU 21は、暗号化復号部24を制御し、コンテンツキーでコンテンツを暗号化させる。コンテンツキーは、コンテンツを取得したとき、同時に取得されたものである (図5または図19)。

【0141】次に、ステップ S 177において、CPU 21は、ファイルフォーマットに基づき、データを、例えば、ミニディスク等により構成される光磁気ディスク43に記録させる。

【0142】なお、記録媒体がミニディスクである場合、ステップ S 176において、CPU 21は、コンテンツをコーデック部25に供給し、例えば、ATRAC3方式によりコンテンツを符号化させる。そして、符号化されたデータが暗号化復号部24によりさらに暗号化される。

【0143】図24は、以上のようにして、記録媒体にコンテンツが記録された状態を模式的に表している。暗号化されているコンテンツ (E (At3)) から抽出されたウォーターマーク (WM) が、コンテンツの外 (ヘッダ) に記録されている。

【0144】図25は、コンテンツを記録媒体に記録する場合のファイルフォーマットのより詳細な構成を表している。この例においては、コンテンツID (CID)、ライセンスID (LID)、URL、およびウォーターマーク (WM) を含むヘッダが記録されている他、EKB、コンテンツキーKcをルートキーKRで暗号化したデータ (Enc (KR, Kc))、証明書 (Cert)、ヘッダに基づき生成されたデジタル署名 (Sig (Header))、コンテンツをコンテンツキーKcで暗号化したデータ (Enc (Kc, Content))、メタデータ (Meta Data) およびマーク (Mark) が記録されている。

【0145】ウォーターマークは、コンテンツの内部に埋め込まれているものであるが、図24と図25に示されるように、コンテンツの内部とは別に、ヘッダ内に配

置するようにすることで、ウォーターマークとしてコンテンツに埋め込まれている情報を迅速に、かつ簡単に検出することが可能となる。従って、そのコンテンツを、コピーすることができるか否かを、迅速に判定することができる。

【0146】なお、メタデータは、例えば、ジャケット、写真、歌詞等のデータを表す。マークについては、図31を参照して後述する。

【0147】図26は、証明書としての公開鍵証明書の例を表している。公開鍵証明書は、通常、公開鍵暗号方式における認証局 (CA: Certificate Authority) が発行する証明書であり、ユーザが、認証局に提出した自己のIDや公開鍵などに、認証局が有効期限等の情報を付加し、さらに、認証局によるデジタル署名を付加して作成される。この発明においては、ライセンスサーバ4 (またはコンテンツサーバ3) が、証明書と秘密鍵、従って公開鍵も発行するので、ユーザは、ユーザID、パスワード等をライセンスサーバ4に提供し登録処理を行うことによって、この公開鍵証明書を得ることができる。

【0148】図26における公開鍵証明書は、証明書のバージョン番号、ライセンスサーバ4が証明書の利用者 (ユーザ) に対して割りつける証明書の通し番号、デジタル署名に用いたアルゴリズム、およびパラメータ、認証局 (ライセンスサーバ4) の名前、証明書の有効期限、証明書利用者のID (ノードIDまたはリーフID)、並びに証明書利用者の公開鍵が、メッセージとして含まれている。さらに、このメッセージには、認証局としてのライセンスサーバ4により作成されたデジタル署名が付加されている。このデジタル署名は、メッセージに対してハッシュ関数を適用して生成されたハッシュ値に基づいて、ライセンスサーバ4の秘密鍵を用いて生成されたデータである。

【0149】ノードIDまたはリーフIDは、例えば、図12の例の場合、デバイス0であれば「0000」とされ、デバイス1であれば「0001」とされ、デバイス15であれば「1111」とされる。このようなIDに基づいて、そのデバイス (エンティティ) がツリー構成のどの位置 (リーフまたはノード) に位置するエンティティであるのかが識別される。

【0150】このように、コンテンツを利用するのに必要なライセンスを、コンテンツとは分離して配布するようにすることにより、コンテンツの配布が自由に行われることになる。任意の方法、あるいは経路で入手されたコンテンツは、一元的に取り扱うことが可能である。

【0151】また、ファイルフォーマットを図25に示されるように構成することで、そのフォーマットのコンテンツを、インターネットを介して配信する場合は勿論、SDMI (Secure Digital Music Initiative) 機器に提供する場合においても、コンテンツの著作権を管理することが可能となる。

【0152】さらに、例えば、図27に示されるように、コンテンツが記録媒体を介して提供されたとしても、インターネット2を介して提供されたとしても、同様の処理により、SDMI (Secure Digital Music Initiative) 機器としての所定のPD (Portable Device) 等に、チェックアウトしたりすることが可能となる。

【0153】次に、図28のフローチャートを参照して、クライアント1が他のクライアント (例えば、PD) に対してコンテンツをチェックアウトする場合の処理について説明する。

【0154】最初に、ステップS191において、CPU21は、コンテンツにデジタル署名が付加されているかを判定する。デジタル署名が付加されていると判定された場合、ステップS192に進み、CPU21は、証明書を出し、認証局 (ライセンスサーバ4) の公開鍵で検証する処理を実行する。すなわち、クライアント1は、ライセンスサーバ4からライセンスサーバ4の秘密鍵に対応する公開鍵を取得し、その公開鍵で公開鍵証明書に付加されているデジタル署名を復号する。図26を参照して説明したように、デジタル署名は、認証局 (ライセンスサーバ4) の秘密鍵に基づいて生成されており、ライセンスサーバ4の公開鍵を用いて復号することができる。さらに、CPU21は、証明書のメッセージ全体に対してハッシュ関数を適用してハッシュ値を演算する。そしてCPU21は、演算されたハッシュ値と、デジタル署名を復号して得られたハッシュ値とを比較し、両者が一致すれば、メッセージは改竄されたものではないと判定する。両者が一致しない場合には、この証明書は、改竄されたものであるということになる。

【0155】そこで、ステップS193において、CPU21は、証明書が改竄されていないかを判定し、改竄されていないと判定された場合、ステップS194に進み、証明書をEKBで検証する処理を実行する。この検証処理は、証明書に含まれるリーフID (図26) に基づいて、EKBをたどることができるかを調べることにより行われる。この検証について、図29と図30を参照して説明する。

【0156】いま、図29に示されるように、例えば、リーフキーK1001を有するデバイスがリポーカされたデバイスであるとする。このとき、図30に示されるようなデータ (暗号化キー) とタグを有するEKBが、各デバイス (リーフ) に配布される。このEKBは、図29におけるデバイス「1001」をリポーカするために、キーKR, K1, K10, K100を更新するEKBとなっている。

【0157】リポーカデバイス「1001」以外の全てのリーフは、更新されたルートキーK(t)Rを取得することができる。すなわち、ノードキーK0の下位に連なるリーフは、更新されていないノードキーK0を、デバイス内に保持しているので、暗号化キーEnc(K0,

K(t)R)を、キーK0によって復号することで、更新ルートキーK(t)Rを取得することができる。

【0158】また、ノードキーK11以下のリーフは、更新されていないノードキーK11を用いて、Enc(K11, K(t)1)をノードキーK11によって復号することで、更新ノードキーK(t)1を取得することができる。さらに、Enc(K(t)1, K(t)R)をノードキーK(t)1によって復号することで、更新ルートキーK(t)Rを取得することが可能となる。ノードキーK101の下位リーフについても、同様に更新ルートキーK(t)Rを取得することが可能である。

【0159】さらに、リポーカされていないリーフキーK1000を有するデバイス「1000」は、自己のリーフキーK1000でEnc(K1000, K(t)100)を復号して、ノードキーK(t)100を取得することができ、これを用いてさらに、上位のノードキーを順次復号し、更新ルートキーK(t)Rを取得することができる。

【0160】これに対して、リポーカされたデバイス「1001」は、自己のリーフの1段上の更新ノードキーK(t)100を、EKB処理により取得できないので、結局、更新ルートキーK(t)Rを取得することができない。

【0161】リポーカされていない正当なデバイス (クライアント1) には、図30に示されるデータとタグを有するEKBが、ライセンスサーバ4から配信され、格納されている。

【0162】そこで、各クライアントは、そのタグを利用して、EKB追跡処理を行うことができる。このEKB追跡処理は、上位のルートキーからキー配信ツリーをたどるか否かを判定する処理である。

【0163】例えば、図29のリーフ「1001」のID (リーフID) である「1001」を、「1」「0」「0」「1」の4ビットとして把握し、最上位ビットから順次、下位ビットに従って、ツリーをたどることができるかが判定される。この判定では、ビットが1であれば、右側に進み、0であれば、左側に進む処理が行われる。

【0164】ID「1001」の最上位ビットが1であるから、図29のルートキーKRから右側に進む。EKBの最初のタグ (番号0のタグ) は、0: {0, 0} であり、両枝にデータを有するものであると判定される。この場合、右側に進むことができるので、ノードキーK1にたどり着くことができる。

【0165】次に、ノードキーK1の下位のノードに進む。ID「1001」の2番目のビットは0であるから左側に進む。番号1のタグは、左側のノードキーK0の下位のデータの有無を表すものであり、ノードキーK1の下位のデータの有無を示すタグは、番号2のタグである。このタグは、図30に示されるように、2: {0,

0) であり、両枝にデータを有するものとされる。従って、左側に進み、ノードキーK10にたどり着くことができる。

【0166】さらに、ID「1001」の3番目のビットは0であり、左側に進む。このとき、K10の下位のデータの有無を示すタグ（番号3のタグ）は、3：{0, 0} であり、両枝にデータを有するものと判定される。そこで、左側に進み、ノードキーK100にたどり着くことができる。

【0167】さらに、ID「1001」の最下位ビットは1であり、右側に進む。番号4のタグは、ノードキーK11に対応するものであり、K100の下位のデータの符号を表すタグは、番号5のタグである。このタグは、5：{0, 1} である。従って、右側には、データが存在しないことになる。その結果、ノード「1001」にはたどり着けないことになり、ID「1001」のデバイスは、EKBによる更新ルートキーを取得できないデバイス、すなわちリボークデバイスであると判定される。

【0168】これに対して、例えば、リーフキーK1000を有するデバイスIDは、「1000」であり、上述した場合と同様に、EKB内のタグに基づくEKB追跡処理を行うと、ノード「1000」にたどり着くことができる。従って、ID「1000」のデバイスは、正当なデバイスであると判定される。

【0169】図28に戻って、CPU21は、ステップS194の検証処理に基づき、証明書がリボークされていないか否かをステップS195で判定し、証明書がリボークされていない場合には、ステップS196に進み、デジタル署名を証明書に含まれる公開鍵で検証する処理を実行する。

【0170】すなわち、図26に示されるように、証明書には、証明書利用者（コンテンツ作成者）の公開鍵が含まれており、この公開鍵を用いて、図25に示される署名（Sig（Header））が検証される。すなわち、この公開鍵を用いて、デジタル署名Sig（Header）を復号して得られたデータ（ハッシュ値）と、図25に示されるHeaderにハッシュ関数を適用して演算されたハッシュ値とを比較することで、両者が一致していれば、Headerが改竄されていないことを確認することができる。これに対して、両者が一致しなければ、Headerは改竄されているということになる。

【0171】ステップS197において、CPU21は、Headerが改竄されているか否かを判定し、改竄されていなければ、ステップS198に進み、ウォーターマークを検証する。ステップS199において、CPU21は、ウォーターマークの検証の結果、チェックアウトが可能であるか否かを判定する。チェックアウトが可能である場合には、ステップS200に進み、CPU21は、チェックアウトを実行する。すなわち、チェックアウト先のクライアント1に対してコンテンツを転送し、コピーさ

せる。

【0172】ステップS191において、デジタル署名が存在しないと判定された場合、ステップS193において、証明書が改竄されていると判定された場合、ステップS195において、証明書をEKBで検証することができなかったと判定された場合、ステップS197において、デジタル署名の検証の結果、ヘッダが改竄されていると判定された場合、または、ステップS199において、ウォーターマークにチェックアウトの禁止が記述されていると判定された場合、ステップS201に進み、エラー処理が実行される。すなわち、この場合には、チェックアウトが禁止される。

【0173】このように、証明書と秘密鍵をライセンスサーバ4からユーザに配布し、コンテンツ作成時に、デジタル署名を付加することにより、コンテンツの作成者の真正を保証することが可能となる。これにより、不正なコンテンツの流通を抑制することができる。

【0174】さらに、ウォーターマークをコンテンツ作成時に検出し、その情報をデジタル署名に付することで、ウォーターマーク情報の改竄を防止し、コンテンツの真正を保証することができる。

【0175】その結果、一度作成されたコンテンツは、どのような形態で配信されたとしても、元のコンテンツの真正を保証することが可能となる。

【0176】さらに、コンテンツは、使用条件を有さず、使用条件は、ライセンスに付加されているので、ライセンス内の使用条件を変更することで、それに関するコンテンツの使用条件を一斉に変更することが可能となる。

【0177】次に、マークの利用方法について説明する。本発明においては、上述したように、使用条件は、コンテンツではなく、ライセンスに付加される。しかしながら、コンテンツによって、使用状況が異なる場合がある。そこで、本発明においては、図25に示されるように、コンテンツにマークが付加される。

【0178】ライセンスとコンテンツは、1対多の関係にあるため、コンテンツの個々の使用状況をライセンスの使用条件にのみ記述するのは困難となる。そこで、このように、コンテンツに使用状況を付加することにより、ライセンスでの管理をしながらも、個々のコンテンツを管理することが可能となる。

【0179】このマークには、例えば、図31に示されるように、ユーザのID（リーフID）、所有権フラグ、使用開始時刻、およびコピー回数等が記述される。

【0180】さらに、マークには、リーフID、所有権フラグ、使用開始時刻、およびコピー回数等のメッセージに基づいて生成されたデジタル署名が付加される。

【0181】所有権フラグは、例えば、所定の期間だけコンテンツを使用可能とするライセンスを、そのまま買い取ったような場合（使用期間を永久に変更したような

場合)に付加される。使用開始時刻は、コンテンツの使用を所定の期間内に開始した場合に記述される。例えば、コンテンツをダウンロードする時期が制限されているような場合において、その期限内にダウンロードが行われたようなとき、その実際にコンテンツをダウンロードした日時がここに記述される。これにより、期間内での有効な使用であることが、証明される。

【0182】コピー回数には、それまでにそのコンテンツをコピーした回数が履歴(ログ)として記述される。

【0183】次に、図32のフローチャートを参照して、ユーザがライセンスを買い取った場合に、マークを付加する処理について、マークをコンテンツに付加する例として説明する。

【0184】最初に、ステップS221において、CPU21は、入力部26からのユーザの指令に基づいて、インターネット2を介して、ライセンスサーバ4にアクセスする。

【0185】ステップS222において、CPU21は、ユーザからの入力部26を介しての入力を取り込み、その入力に対応してライセンスサーバ4に対してライセンスの買い取りを要求する。

【0186】この要求に対応して、図33のフローチャートを参照して後述するように、ライセンスサーバ4は、ライセンスを買い取るために必要な対価を提示してくる(図33のステップS242)。そこで、ステップS223において、クライアント1のCPU21は、ライセンスサーバ4からの対価の提示を受け取ると、これを出力部27に出力し、表示させる。

【0187】ユーザは、この表示に基づいて、提示された対価を了承するか否かを判断し、その判断結果に基づいて、入力部26からその判断結果を入力する。

【0188】CPU21は、ステップS224において、入力部26からの入力に基づいて、ユーザが提示された対価を了承したか否かを判定し、了承したと判定した場合には、ステップS225に進み、ライセンスサーバ4に了承を通知する処理を実行する。

【0189】この了承通知を受信すると、ライセンスサーバ4は、対価の買い取りを表す情報、すなわち所有権フラグを記述したマークを送信してくる(図33のステップS244)。そこで、ステップS226において、クライアント1のCPU21は、ライセンスサーバ4からのマークを受け取ると、ステップS227において、受け取ったマークをコンテンツに埋め込む処理を実行する。すなわち、これにより、買い取られたライセンスに対応するコンテンツのマークとして、図31に示されるような所有権フラグが記述されたマークがコンテンツに対応して記録されることになる。また、このとき、CPU21は、メッセージが更新されたことになるので、デジタル署名(図25)も更新し、記録媒体に記録する。

【0190】ステップS224において、ライセンスサ

サーバ4から提示された対価が了承されていないと判定された場合、ステップS228に進み、CPU21は、提示された対価を了承しないことをライセンスサーバ4に通知する。

【0191】このようなクライアント1の処理に対応して、ライセンスサーバ4は、図33のフローチャートに示す処理を実行する。

【0192】すなわち、最初に、ステップS241において、ライセンスサーバ4のCPU21は、クライアント1からライセンス買い取りの要求が送信されてくると(図32のステップS222)、これを受け取り、ステップS242において、対象とされているライセンスの買い取りに必要な対価を記憶部28から読み出し、これをクライアント1に送信する。

【0193】上述したように、このようにして提示された対価に対して、クライアント1から提示された対価を了承するか否かの通知が送信されてくる。

【0194】そこで、ステップS243において、ライセンスサーバ4のCPU21は、クライアント1から了承通知を受信したか否かを判定し、了承通知を受信したと判定した場合、ステップS244に進み、対象とされるライセンスの買い取りを表すメッセージを含むマークを生成し、自分自身の秘密鍵で、デジタル署名を付加して、クライアント1に送信する。このようにして送信されたマークは、上述したように、クライアント1の記憶部28において、対応するコンテンツに記録される(図32のステップS227)。

【0195】ステップS243において、クライアント1から了承通知が受信されていないと判定された場合、ステップS244の処理はスキップされる。すなわち、この場合には、ライセンスの買い取り処理が最終的に行われなかったことになるので、マークは送信されない。

【0196】図34は、ステップS244において、ライセンスサーバ4からクライアント1に対して送信されるマークの構成例を表している。この例においては、そのユーザのリーフID、所有権フラグ(Own)、並びにリーフIDと所有権フラグを、ライセンスサーバ4の秘密鍵Sに基づいて生成されたデジタル署名Sigs(LeafID, Own)により、マークが構成されている。

【0197】なお、このマークは、特定のユーザの特定のコンテンツに対してのみ有効なものであるため、対象とされるコンテンツがコピーされた場合には、そのコピーされたコンテンツに付随するマークは無効とされる。

【0198】このようにして、コンテンツとライセンスを分離し、使用条件をライセンスに対応させる場合においても、個々のコンテンツの使用状況に応じたサービスを実現することが可能となる。

【0199】次に、グルーピングについて説明する。複数の機器やメディアを適当に集め、その1つの集合内においては、コンテンツを自由に授受することができるよ

うにすることは、グルーピングと称される。通常、このグルーピングは、個人の所有する機器やメディアにおいて行われる。このグルーピングは、従来、グループ毎にグループキーを設定する等して行われていたが、グループ化する複数の機器やメディアに、同一のライセンスを対応づけることにより、容易にグルーピングすることが可能となる。

【0200】また、各機器を予め登録しておくことで、グルーピングすることも可能である。この場合のグルーピングについて、以下に説明する。

【0201】この場合、ユーザは、グルーピング対象とされる機器の証明書を予めサーバに登録しておく必要がある。この証明書の登録処理について、図35と図36のフローチャートを参照して説明する。

【0202】最初に、図35のフローチャートを参照して、クライアント（グルーピング対象となる機器）の証明書の登録処理について説明する。ステップS261において、クライアント1のCPU21は、グルーピングの対象とされる機器としての自分自身の証明書を作成する。この証明書には、自分自身の公開鍵が含まれる。

【0203】次に、ステップS262に進み、CPU21は、ユーザの入力部26からの入力に基づいて、コンテンツサーバ3にアクセスし、ステップS263において、ステップS261の処理で作成された証明書をコンテンツサーバ3に送信する処理を実行する。

【0204】なお、証明書としては、ライセンスサーバ4から受信したものを、そのまま使用することもできる。

【0205】以上の処理は、グルーピング対象とされる全ての機器が行う。

【0206】次に、図36のフローチャートを参照して、図35のクライアント1の証明書の登録処理に対応して行われるコンテンツサーバ3の証明書の登録処理について説明する。

【0207】最初に、ステップS271において、コンテンツサーバ3のCPU21は、クライアント1から送信されてきた証明書を受信すると、ステップS272において、その証明書を記憶部28に登録する。

【0208】以上の処理が、グループ対象とされる機器毎に行われる。その結果、コンテンツサーバ3の記憶部28には、例えば、図37に示されるように、グループ毎に、そのグループを構成するデバイスの証明書が登録される。

【0209】図37に示される例では、グループ1の証明書として、証明書C11乃至C14が登録されている。これらの証明書C11乃至C14には、対応する公開鍵Kp11乃至Kp14が含まれている。

【0210】同様に、グループ2の証明書として、証明書C21乃至C23が登録されており、これらに対応する公開鍵Kp21乃至Kp23が含まれている。

【0211】以上のようなグループを構成する各機器毎に、その証明書が登録された状態において、ユーザからそのグループに属する機器にコンテンツの提供が要求されると、コンテンツサーバ3は、図38のフローチャートに示す処理を実行する。

【0212】最初に、ステップS281において、コンテンツサーバ3のCPU21は、記憶部28に記憶されている証明書のうち、そのグループに属する証明書を検証する処理を実行する。

10 【0213】この検証処理は、図29と図30を参照して説明されたように、各機器の証明書に含まれるリーフIDに基づいて、タグを利用してEKBをたどることで行われる。EKBは、コンテンツサーバ3にも、ライセンスサーバ4から配布されている。この検証処理により、リボークされている証明書は除外される。

20 【0214】ステップS282において、コンテンツサーバ3のCPU21は、ステップS281の検証処理の結果、有効とされた証明書を選択する。そして、ステップS283において、CPU21は、ステップS282の処理で選択された各機器の証明書の各公開鍵でコンテンツ鍵を暗号化する。ステップS284において、CPU21は、対象とされるグループの各機器に、ステップS283の処理で暗号化されたコンテンツ鍵をコンテンツとともに送信する。

【0215】図37に示されるグループ1のうち、例えば、証明書C14がリボークされているとすると、ステップS283の処理で、例えば、図39に示されるような暗号化データが生成される。

30 【0216】すなわち、図39の例においては、コンテンツ鍵Kcが、証明書C11の公開鍵Kp11、証明書C12の公開鍵Kp12、または証明書C13の公開鍵Kp13により、暗号化されている。

【0217】コンテンツサーバ3の図38に示されるような処理に対応して、コンテンツの提供を受ける各グループの機器（クライアント）は、図40のフローチャートに示す処理を実行する。

40 【0218】最初に、ステップS291において、クライアント1のCPU21は、コンテンツサーバ3が図38のステップS284の処理で送信してきたコンテンツを、コンテンツ鍵とともに受信する。コンテンツは、コンテンツ鍵Kcにより、暗号化されており、コンテンツ鍵は上述したように、各機器が保持する公開鍵により暗号化されている（図39）。

【0219】そこで、ステップS292において、CPU21は、ステップS291の処理で受信した自分宛のコンテンツ鍵を、自分自身の秘密鍵で復号し、取得する。そして、取得したコンテンツ鍵を用いてコンテンツの復号処理が行われる。

50 【0220】例えば、図39の例に示される証明書C11に対応する機器は、公開鍵Kp11に対応する自分自身

の秘密鍵を用いて、コンテンツ鍵Kcの暗号を復号し、コンテンツ鍵Kcを取得する。そして、コンテンツ鍵Kcを用いて、コンテンツがさらに復号される。

【0221】同様の処理は、証明書C12、C13に対応する機器においても行われる。リポークされている証明書C14の機器は、自分自身の公開鍵を用いて暗号化されたコンテンツ鍵Kcがコンテンツに付随して送られてこないの、コンテンツ鍵Kcを復号することができず、従って、コンテンツ鍵Kcを用いてコンテンツを復号することができない。

【0222】以上においては、コンテンツキー（すなわちコンテンツ）に対してグルーピングを行うようにしたが、ライセンスキー（ライセンス）に対してグルーピングを行うことも可能である。

【0223】以上のようにして、特別なグループキーや、後述するICV（Integrity Check Value）を用いずにグループ化が可能となる。このグループ化は、小規模のグループに適用するのに向いている。

【0224】本発明においては、ライセンスもチェックアウト、あるいはチェックインしたり、ムーブしたり、コピーしたりすることが可能とされる。但し、これらの処理はSDMIで定められたルールに基づいて行われる。

【0225】次に、図41と図42のフローチャートを参照して、このようなクライアントによるライセンスのチェックアウト処理について説明する。

【0226】最初に、図41のフローチャートを参照して他のクライアントにライセンスをチェックアウトするクライアントの処理について説明する。最初に、ステップS301において、クライアント1のCPU21は、チェックアウト対象のライセンスのチェックアウト回数N1を読み取る。このチェックアウト回数は、図8に示される使用条件に書き込まれているので、この使用条件から読み取られる。

【0227】次に、ステップS302において、CPU21は、チェックアウト対象のライセンスの最大チェックアウト回数N2を、やはりライセンスの使用条件から読み取る。

【0228】そして、ステップS303において、CPU21は、ステップS301の処理で読み取られたチェックアウト回数N1と、ステップS302の処理で読み取られた最大チェックアウト回数N2とを比較し、チェックアウト回数N1が最大チェックアウト回数N2より大きいかなかを判定する。

【0229】チェックアウト回数N1が、最大チェックアウト回数N2より小さいと判定された場合、ステップS304に進み、CPU21は、相手側の装置（チェックアウト先のクライアント）のリーフキーを相手個々の装置から取得し、そのリーフキーを、いまチェックアウト対象とされているライセンスIDに対応して記憶部28のチェックアウトリストに記憶させる。

【0230】次に、ステップS305において、CPU21は、ステップS301の処理で読み取られたライセンスのチェックアウト回数N1の値を1だけインクリメントする。ステップS306において、CPU21は、ライセンスのメッセージに基づいて、ICVを演算する。このICVについては、図46乃至図50を参照して後述する。ICVを用いてライセンスの改竄を防止することが可能となる。

【0231】次に、ステップS307において、CPU21は、チェックアウト対象のライセンスと、ステップS306の処理で演算されたICVを、自分自身の公開鍵を用いて暗号化して、EKBおよび証明書とともに、相手側の装置に出力し、コピーさせる。さらに、ステップS308において、CPU21は、ステップS306の処理で演算されたICVを、相手側装置のリーフキーと、ライセンスIDに対応して記憶部28のチェックリスト中に記憶させる。

【0232】ステップS303において、チェックアウト回数N1が最大チェックアウト回数N2より小さくない（例えば、等しい）と判定された場合、もはや許容される回数だけチェックアウトが行われているので、これ以上チェックアウトを行うことができない。そこで、ステップS309に進み、CPU21は、エラー処理を実行する。すなわち、この場合、チェックアウト処理は実行されないことになる。

【0233】次に、図42のフローチャートを参照して、図41のチェックアウト処理により、ライセンスのチェックアウトを受けるクライアントの処理について説明する。

【0234】最初に、ステップS321において、相手側装置（ライセンスをチェックアウトするクライアント1）に、自分自身のリーフキーを送信する。このリーフキーは、ステップS304において、相手側のクライアントにより、ライセンスIDに対応して記憶される。

【0235】次に、ステップS322において、CPU21は、相手側のクライアント1から暗号化されたライセンスとICVが、EKBおよび証明書とともに送信されてきた場合、これを受信する。すなわち、このライセンス、ICV、EKBおよび証明書は、図41のステップS307の処理で相手側の装置から送信されたものである。

【0236】ステップS323において、CPU21は、ステップS322の処理で受信したライセンス、ICV、EKBおよび証明書を、記憶部28に記憶させる。

【0237】以上のようにして、ライセンスのチェックアウトを受けたクライアント1は、チェックアウトを受けたそのライセンスを使用して、所定のコンテンツを再生する場合、図43のフローチャートに示される処理を実行する。

【0238】すなわち、最初に、ステップS341において、クライアント1のCPU21は、ユーザより入力部

26を介して再生が指定されたコンテンツのICVを演算する。そして、ステップS342において、CPU21は、記憶部28に記憶されている暗号化されているICVを、証明書に含まれている公開鍵に基づいて、復号させる。

【0239】次に、ステップS343において、CPU21は、ステップS341の処理により、いま演算されたICVと、ステップS342の処理により読み出され、復号されたICVが一致するかどうかを判定する。両者が一致する場合には、ライセンスは改竄されていないことになる。そこで、ステップS344にすすみ、CPU21は、対応するコンテンツを再生する処理を実行する。

【0240】これに対して、ステップS343において、2つのICVが一致しないと判定された場合、ライセンスは改竄されている恐れがある。このため、ステップS345に進み、CPU21は、エラー処理を実行する。すなわち、このとき、そのライセンスを用いてコンテンツを再生することができないことになる。

【0241】次に、以上のようにして、他のクライアントに一旦チェックアウトしたライセンスのチェックインを受けるクライアントの処理について、図44のフローチャートを参照して説明する。

【0242】最初に、ステップS361において、CPU21は、相手側の装置（ライセンスを返却（チェックイン）してくるクライアント1）のリーフキーと、チェックイン対象のライセンスのIDを取得する。次に、ステップS362において、CPU21は、ステップS361で取得されたチェックイン対象のライセンスが、自分自身が相手側装置にチェックアウトしたライセンスであるかどうかを判定する。この判定は、図41のステップS308の処理で記憶されたICV、リーフキー、およびライセンスIDに基づいて行われる。すなわち、ステップS361で取得されたリーフキー、ライセンスID、およびICVが、チェックアウトリスト中に記憶されているかどうか判定され、記憶されている場合には、自分自身がチェックアウトしたライセンスであると判定される。

【0243】ライセンスが、自分自身がチェックアウトしたものであるとき、ステップS363において、CPU21は、相手側の装置のライセンス、EKBおよび証明書の削除を要求する。後述するように、この要求に基づいて、相手側の装置は、ライセンス、EKBおよび証明書の削除を実行する（図45のステップS383）。

【0244】ステップS364において、CPU21は、一旦チェックアウトしたライセンスが再びチェックインされてきたので、そのライセンスのチェックアウト回数N1を1だけデクリメントする。

【0245】ステップS365において、CPU21は、相手側の装置に他のライセンスをチェックアウトしているかどうかを判定し、まだチェックアウトしている他のライセンスが存在しない場合には、ステップS366に進

み、CPU21は、相手側の装置のチェックイン対象機器としてのチェックアウトリストにおける記憶を削除する。これに対して、ステップS365において、相手側の装置にチェックアウトしている他のライセンスが存在すると判定された場合には、他のライセンスのチェックインを受ける可能性があるので、ステップS366の処理はスキップされる。

【0246】ステップS362において、チェックイン対象とされているライセンスが、自分自身が相手側装置にチェックアウトしたライセンスではないと判定された場合、CPU21は、ステップS367に進み、エラー処理を実行する。すなわち、この場合には、自分自身が管轄するライセンスではないことになるので、チェックイン処理は実行されない。

【0247】ユーザが、ライセンスを不正にコピーしたような場合、記憶されているICVの値と、ステップS361の処理で取得されたライセンスに基づいて演算されたICVの値が異なるものとなるので、チェックインできないことになる。

【0248】図45は、図44のフローチャートに示されるライセンスのチェックイン処理を実行するクライアントに対して、自分自身が有しているライセンスをチェックインさせるクライアントの処理を表している。

【0249】ステップS381において、クライアント1のCPU21は、相手側の装置（図44のフローチャートに示す処理を実行するクライアント1）にリーフキーとチェックイン対象のライセンスのIDを送信する。上述したように、相手側の装置は、ステップS361において、このリーフキーとライセンスIDを取得し、ステップS362において、それに基づいて、チェックイン対象のライセンスの認証処理を実行する。

【0250】ステップS382において、クライアント1のCPU21は、相手側の装置からライセンスの削除を要求されたかどうかを判定する。すなわち、ライセンスが正当なチェックイン対象のライセンスである場合、上述したように、相手側の装置は、ステップS363の処理でライセンス、EKBおよび証明書の削除を要求してくる。そこで、この要求を受信した場合、ステップS383に進み、CPU21は、ライセンス、EKBおよび証明書を削除する。すなわち、これにより、このクライアント1は、以後そのライセンスを使用できない状態となり、図44のステップS364の処理により、チェックアウト回数N1が、1だけデクリメントされるので、チェックインが完了したことになる。

【0251】ステップS382において、相手側の装置からライセンスの削除が要求されていないと判定された場合、ステップS384に進み、エラー処理が実行される。すなわち、この場合には、ICVの値が異なっている等の理由により、チェックインができないことになる。

【0252】以上においては、チェックインとチェック

アウトについて説明したが、同様に、ライセンスをコピーあるいはムーブさせるようにすることも可能である。

【0253】次に、ライセンス（コンテンツも同様）の改竄を防止するためにライセンスのインテグリティ・チェック値（ICV）を生成して、ライセンスに対応付けて、ICVの計算により、ライセンス改竄の有無を判定する処理構成について説明する。

【0254】ライセンスのインテグリティ・チェック値（ICV）は、例えばライセンスに対するハッシュ関数を用いて計算され、 $ICV = hash(Kicv, L1, L2, \dots)$  によって計算される。KicvはICV生成キーである。L1, L2はライセンスの情報であり、ライセンスの重要情報のメッセージ認証符号（MAC: Message authentication Code）が使用される。

【0255】DES暗号処理構成を用いたMAC値生成例を図46に示す。図46の構成に示すように対象となるメッセージを8バイト単位に分割し、（以下、分割されたメッセージをM1、M2、・・・、MNとする）、まず、初期値（IV）とM1を、演算部24-1Aにより排他的論理和する（その結果をI1とする）。次に、I1をDES暗号化部24-1Bに入れ、鍵（以下、K1とする）を用いて暗号化する（出力をE1とする）。続けて、E1およびM2を演算部24-2Aにより排他的論理和し、その出力I2をDES暗号化部24-2Bへ入れ、鍵K1を用いて暗号化する（出力E2）。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。DES暗号化部24-NBから最後に出てきたENがメッセージ認証符号（MAC（Message Authentication Code））となる。

【0256】このようなライセンスのMAC値とICV生成キーにハッシュ関数を適用してライセンスのインテグリティ・チェック値（ICV）が生成される。例えばライセンス生成時に生成したICVと、新たにライセンスに基づいて生成したICVとを比較して同一のICVが得られればライセンスに改竄のないことが保証され、ICVが異なれば、改竄があったと判定される。

【0257】次に、ライセンスのインテグリティ・チェック値（ICV）生成キーであるKicvを上記の有効化キープブロックによって送付する構成について説明する。すなわちEKBによる暗号化メッセージデータをライセンスのインテグリティ・チェック値（ICV）生成キーとした例である。

【0258】図47および図48に複数のデバイスに共通のライセンスを送付した場合、それらのライセンスの改竄の有無を検証するためのインテグリティ・チェック値生成キーKicvを有効化キープブロック（EKB）によって配信する構成例を示す。図47はデバイス0, 1, 2, 3に対して復号可能なチェック値生成キーKicvを配信する例を示し、図48はデバイス0, 1, 2, 3中のデバイス3をリボーク（排除）してデバイス

0, 1, 2に対してのみ復号可能なチェック値生成キーKicvを配信する例を示す。

【0259】図47の例では、更新ノードキーK(t)00によって、チェック値生成キーKicvを暗号化したデータEnc(K(t)00, Kicv)とともに、デバイス0, 1, 2, 3においてそれぞれの有するノードキー、リーフキーを用いて更新されたノードキーK(t)00を復号可能な有効化キープブロック（EKB）を生成して配信する。それぞれのデバイスは、図47の右側に示すように、まず、EKBを処理（復号）することにより、更新されたノードキーK(t)00を取得し、次に、取得したノードキーK(t)00を用いて、暗号化されたチェック値生成キーEnc(K(t)00, Kicv)を復号して、チェック値生成キーKicvを得ることが可能となる。

【0260】その他のデバイス4, 5, 6, 7・・・は同一の有効化キープブロック（EKB）を受信しても自身の保有するノードキー、リーフキーでは、EKBを処理して更新されたノードキーK(t)00を取得することができないので、安全に正当なデバイスに対してのみチェック値生成キーを送付することができる。

【0261】一方、図48の例は、図12の点線枠で囲んだグループにおいてデバイス3が、例えば鍵の漏洩によりリボーク（排除）されているとして、他のグループのメンバ、すなわち、デバイス0, 1, 2, に対してのみ復号可能な有効化キープブロック（EKB）を生成して配信した例である。図48に示す有効化キープブロック（EKB）と、チェック値生成キー（Kicv）をノードキー（K(t)00）で暗号化したデータEnc(K(t)00, Kicv)を配信する。

【0262】図48の右側には、復号手順を示してある。デバイス0, 1, 2は、まず、受信した有効化キープブロックから自身の保有するリーフキーまたはノードキーを用いた復号処理により、更新ノードキー（K(t)00）を取得する。次に、K(t)00による復号によりチェック値生成キーKicvを取得する。

【0263】図12に示す他のグループのデバイス4, 5, 6・・・は、この同様のデータ（EKB）を受信したとしても、自身の保有するリーフキー、ノードキーを用いて更新ノードキー（K(t)00）を取得することができない。同様にリボークされたデバイス3においても、自身の保有するリーフキー、ノードキーでは、更新ノードキー（K(t)00）を取得することができず、正当な権利を有するデバイスのみがチェック値生成キーを復号して利用することが可能となる。

【0264】このように、EKBを利用したチェック値生成キーの配送を用いれば、データ量を少なくして、かつ安全に正当権利者のみが復号可能としたチェック値生成キーを配信することが可能となる。

【0265】このようなライセンスのインテグリティ・

チェック値(ICV)を用いることにより、EKBと暗号化ライセンスの不正コピーを排除することができる。例えば図49Aに示すように、ライセンスL1とライセンスL2とをそれぞれのライセンスキーを取得可能な有効化キーブロック(EKB)とともに格納したメディア1があり、これをそのままメディア2にコピーした場合を想定する。EKBと暗号化ライセンスのコピーは可能であり、これをEKBを復号可能なデバイスでは利用できることになる。

【0266】図49Bに示す例では、各メディアに正当に格納されたライセンスに対応付けてインテグリティ・チェック値(ICV(L1, L2))を格納する構成とする。なお、(ICV(L1, L2))は、ライセンスL1とライセンスL2にハッシュ関数を用いて計算されるライセンスのインテグリティ・チェック値である $ICV = hash(Kicv, L1, L2)$ を示している。図49Bの構成において、メディア1には正当にライセンス1とライセンス2が格納され、ライセンスL1とライセンスL2に基づいて生成されたインテグリティ・チェック値(ICV(L1, L2))が格納される。また、メディア2には正当にライセンス1が格納され、ライセンスL1に基づいて生成されたインテグリティ・チェック値(ICV(L1))が格納される。

【0267】この構成において、メディア1に格納された{EKB, ライセンス2}をメディア2にコピーしたとすると、メディア2で、ライセンスチェック値を新たに生成すると、ICV(L1, L2)が生成されることになり、メディア2に格納されているKicv(L1)と異なり、ライセンスの改竄あるいは不正なコピーによる新たなライセンスの格納が実行されたことが明らかになる。メディアを再生するデバイスにおいて、再生ステップの前ステップにICVチェックを実行して、生成ICVと格納ICVの一致を判別し、一致しない場合は、再生を実行しない構成とすることにより、不正コピーのライセンスの再生を防止することが可能となる。

【0268】また、さらに、安全性を高めるため、ライセンスのインテグリティ・チェック値(ICV)を書き換えカウンタを含めたデータに基づいて生成する構成としてもよい。すなわち $ICV = hash(Kicv, counter+1, L1, L2, \dots)$ によって計算する構成とする。ここで、カウンタ(counter+1)は、ICVの書き換えごとに1つインクリメントされる値として設定する。なお、カウンタ値はセキュアなメモリに格納する構成とすることが必要である。

【0269】さらに、ライセンスのインテグリティ・チェック値(ICV)をライセンスと同一メディアに格納することができない構成においては、ライセンスのインテグリティ・チェック値(ICV)をライセンスとは別のメディア上に格納する構成としてもよい。

【0270】例えば、読み込み専用メディアや通常のM

O等のコピー防止策のとられていないメディアにライセンスを格納する場合、同一メディアにインテグリティ・チェック値(ICV)を格納するとICVの書き換えが不正なユーザによりなされる可能性があり、ICVの安全性が保てないおそれがある。このような場合、ホストマシン上の安全なメディアにICVを格納して、ライセンスのコピーコントロール(例えばcheck-in/check-out、move)にICVを使用する構成とすることにより、ICVの安全な管理およびライセンスの改竄チェックが可能となる。

【0271】この構成例を図50に示す。図50では読み込み専用メディアや通常のMO等のコピー防止策のとられていないメディア2201にライセンス1乃至ライセンス3が格納され、これらのライセンスに関するインテグリティ・チェック値(ICV)を、ユーザが自由にアクセスすることの許可されないホストマシン上の安全なメディア2202に格納し、ユーザによる不正なインテグリティ・チェック値(ICV)の書き換えを防止した例である。このような構成として、例えばメディア2201を装着したデバイスが、メディア2201の再生を実行する際にホストマシンであるPC、サーバにおいてICVのチェックを実行して再生の可否を判定する構成とすれば、不正なコピーライセンスあるいは改竄ライセンスの再生を防止できる。

【0272】本発明が適用されるクライアントは、いわゆるパーソナルコンピュータ以外に、PDA(Personal Digital Assistants)、携帯電話機、ゲーム端末機などすることができる。

【0273】一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、ネットワークや記録媒体からインストールされる。

【0274】この記録媒体は、図2に示されるように、装置本体とは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク41(フロッピーディスクを含む)、光ディスク42(CD-ROM(Compact Disk - ReadOnly Memory)、DVD(Digital Versatile Disk)を含む)、光磁気ディスク43(MD(Mini-Disk)を含む)、もしくは半導体メモリ44などよりなるパッケージメディアにより構成されるだけでなく、装置本体に予め組み込まれた状態でユーザに提供される、プログラムが記録されているROM22や、記憶部28に含まれるハードディスクなどで構成される。

【0275】なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に

実行される処理をも含むものである。

【0276】また、セキュリティに関連する処理を実行させるプログラムは、その処理を解析されるのを防ぐため、そのプログラム自体が暗号化されているのが望ましい。例えば、暗号処理などを行う処理については、そのプログラムをタンパーレジスタントモジュールとして構成することができる。

【0277】また、コンテンツを利用許可するライセンスを特定するためにコンテンツのヘッダに記載されている情報はライセンスを一意に識別するライセンスIDでなくてもよい。上記の実施例では、ライセンスIDが、コンテンツの利用に必要なライセンスを特定する情報であり、あるライセンスが利用を許可するコンテンツを特定する情報であり、クライアント1からライセンス要求によって要求されるライセンスを識別する情報である。コンテンツにコンテンツのそのコンテンツに関する各種属性情報のリストが記載され、ライセンスに、そのライセンスによって利用許可されるコンテンツの条件式を記載するようにしても良い。この場合では、コンテンツに含まれる属性情報がそのコンテンツの利用を許可するライセンスを特定する情報であり、ライセンスに含まれる条件式がそのライセンスが利用を許可するコンテンツを特定する情報であり、ライセンスIDはライセンスを一意に識別する情報となる。このようにした場合には、一つのコンテンツに複数のライセンスを対応付けることが可能になり、ライセンスの発行を柔軟に行うことができる。

【0278】また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

#### 【0279】

【発明の効果】以上の如く、本発明の情報処理装置および方法、ライセンスサーバ、並びにプログラムによれば、暗号化されたデータを自由に配布できるようにし、別途ライセンスを取得することでコンテンツを利用できるようにしたことで、コンテンツの流通を妨げることなく、著作権を保護し、適切な使用料の徴収をすることができる。

#### 【図面の簡単な説明】

【図1】本発明を適用したコンテンツ提供システムの構成を示すブロック図である。

【図2】図1のクライアントの構成を示すブロック図である。

【図3】図1のクライアントのコンテンツのダウンロード処理を説明するフローチャートである。

【図4】図1のコンテンツサーバのコンテンツ提供処理を説明するフローチャートである。

【図5】図4のステップS26におけるフォーマットの例を示す図である。

【図6】図1のクライアントのコンテンツ再生処理を説

明するフローチャートである。

【図7】図6のステップS43のライセンス取得処理の詳細を説明するフローチャートである。

【図8】ライセンスの構成を示す図である。

【図9】図1のライセンスサーバのライセンス提供の処理を説明するフローチャートである。

【図10】図6のステップS45におけるライセンス更新処理の詳細を説明するフローチャートである。

10 【図11】図1のライセンスサーバのライセンス更新処理を説明するフローチャートである。

【図12】キーの構成を説明する図である。

【図13】カテゴリノードを説明する図である。

【図14】ノードとデバイスの対応の具体例を示す図である。

【図15】有効化キーブロックの構成を説明する図である。

【図16】有効化キーブロックの利用を説明する図である。

20 【図17】有効化キーブロックのフォーマットの例を示す図である。

【図18】有効化キーブロックのタグの構成を説明する図である。

【図19】DNKを用いたコンテンツの復号処理を説明する図である。

【図20】有効化キーブロックの例を示す図である。

【図21】複数のコンテンツの1つのデバイスに対する割り当てを説明する図である。

【図22】ライセンスのカテゴリを説明する図である。

30 【図23】クライアントのリッピング処理を説明するフローチャートである。

【図24】ウォーターマークの構成を説明する図である。

【図25】コンテンツのフォーマットの例を示す図である。

【図26】公開鍵証明書の例を示す図である。

【図27】コンテンツの配布を説明する図である。

【図28】クライアントのコンテンツのチェックアウト処理を説明するフローチャートである。

40 【図29】タグによる有効化キーブロックをたどる例を説明する図である。

【図30】有効化キーブロックの構成例を示す図である。

【図31】マークの構成を説明する図である。

【図32】クライアントのライセンス買い取り処理を説明するフローチャートである。

【図33】ライセンスサーバのライセンス買い取り処理を説明するフローチャートである。

【図34】マークの構成例を示す図である。

50 【図35】クライアントの証明書の登録処理を説明するフローチャートである。

【図36】コンテンツサーバの証明書登録処理を説明するフローチャートである。

【図37】グループの証明書の例を示す図である。

【図38】グルーピングが行われている場合におけるコンテンツサーバの処理を説明するフローチャートである。

【図39】コンテンツキーの暗号化の例を示す図である。

【図40】グループに属するクライアントの処理を説明するフローチャートである。

【図41】他のクライアントにライセンスをチェックアウトするクライアントの処理を説明するフローチャートである。

【図42】他のクライアントからライセンスのチェックアウトを受けるクライアントの処理を説明するフローチャートである。

【図43】ライセンスのチェックアウトを受けたクライアントの再生処理を説明するフローチャートである。

【図44】他のクライアントからライセンスのチェックインを受けるクライアントの処理を説明するフローチャートである。

ートである。

【図45】他のクライアントにライセンスをチェックインするクライアントの処理を説明するフローチャートである。

【図46】MACの生成を説明する図である。

【図47】ICV生成キーの復号処理を説明するフローチャートである。

【図48】ICV生成キーの他の復号処理を説明する図である。

10 【図49】ICVによるライセンスのコピーの管理を説明する図である。

【図50】ライセンスの管理を説明する図である。

【符号の説明】

1-1, 1-2 クライアント, 2 インターネット, 3 コンテンツサーバ, 4 ライセンスサーバ, 5 課金サーバ, 20 タイマ, 21 CPU, 24 暗号化復号部, 25 コーデック部, 26 入力部, 27 出力部, 28 記憶部, 29 通信部

【図1】

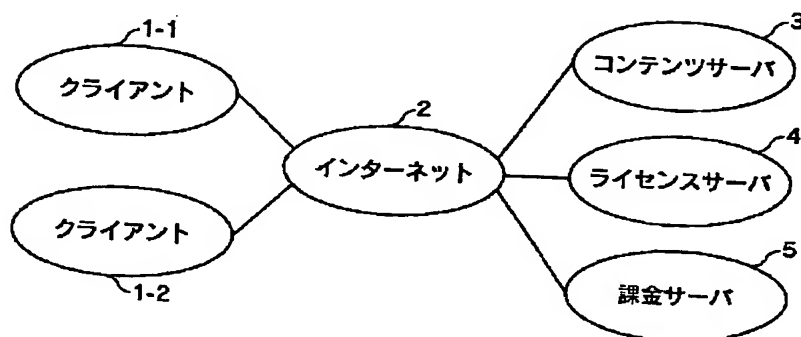


図1

【図3】

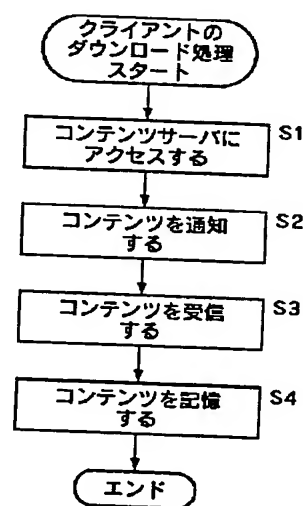


図3

【図8】

ライセンスID
作成日時
有効期限
使用条件
リーフID
電子署名

ライセンス

図8

【図20】

EKB

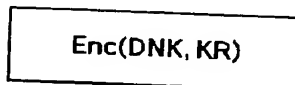


図20

【図2】

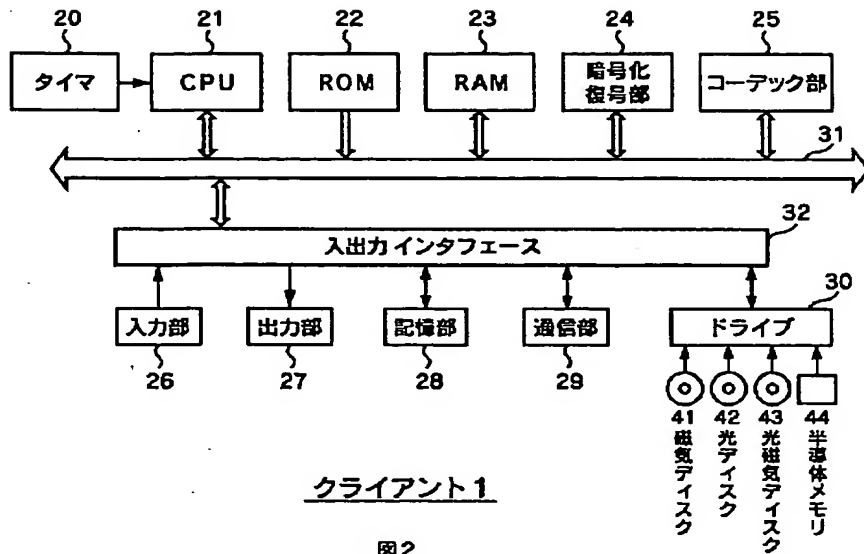


図2

【図4】

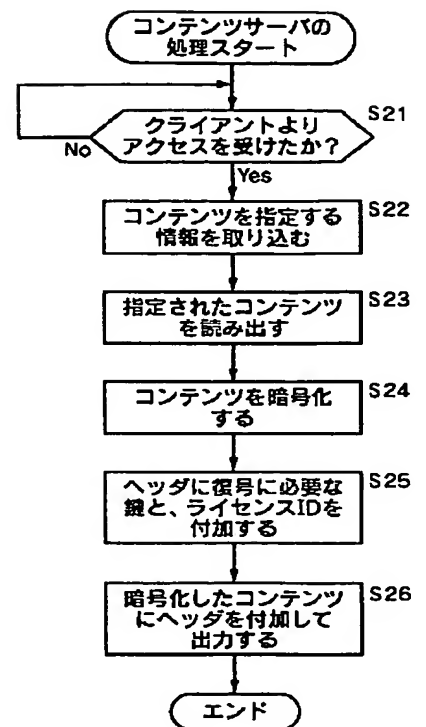


図4

【図5】

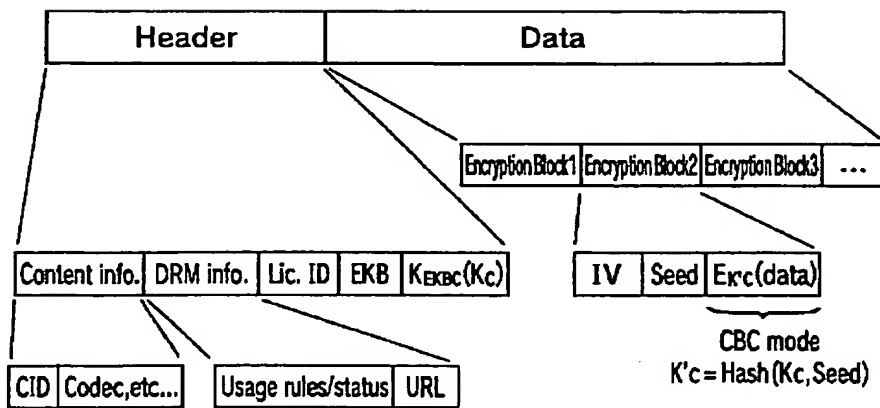


図5

【図11】

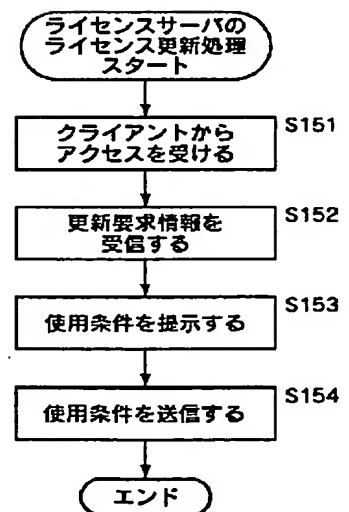


図11

【図6】

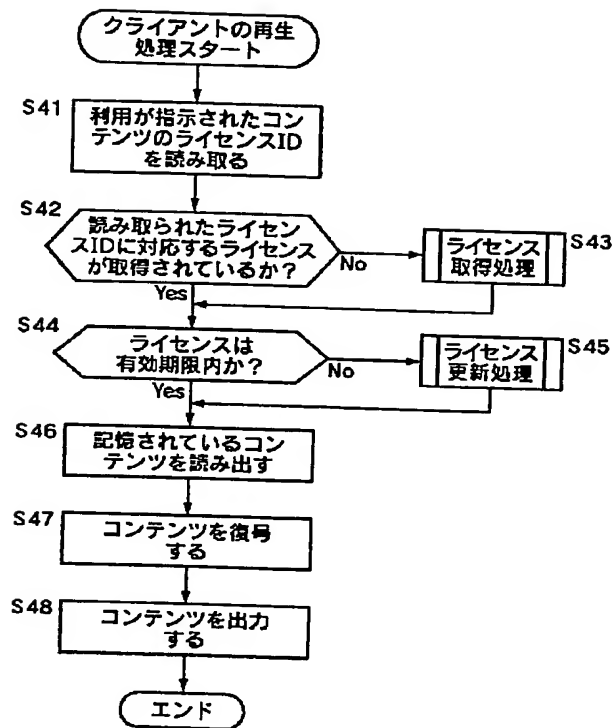


図6

【図7】

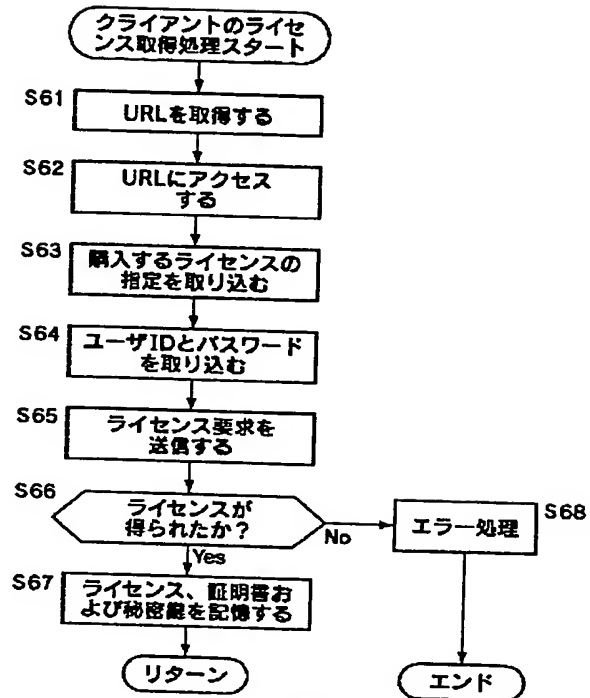


図7

【図12】

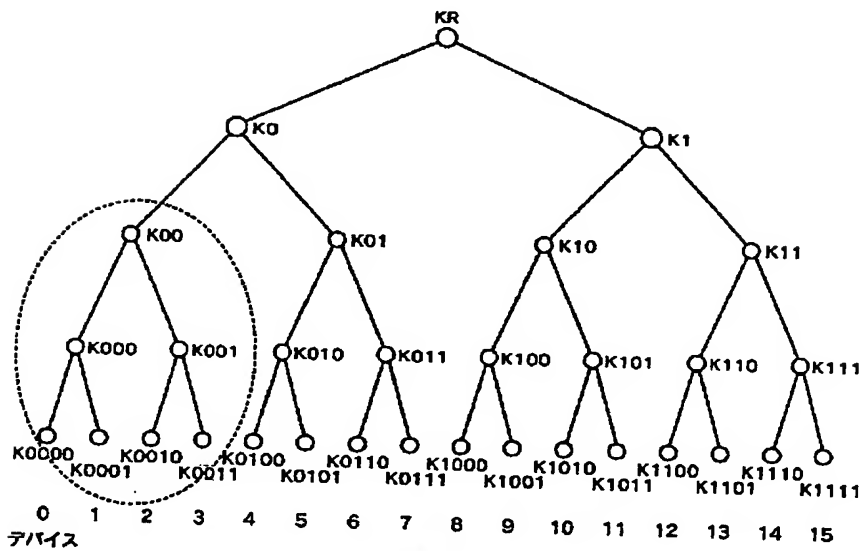


図12

【図23】

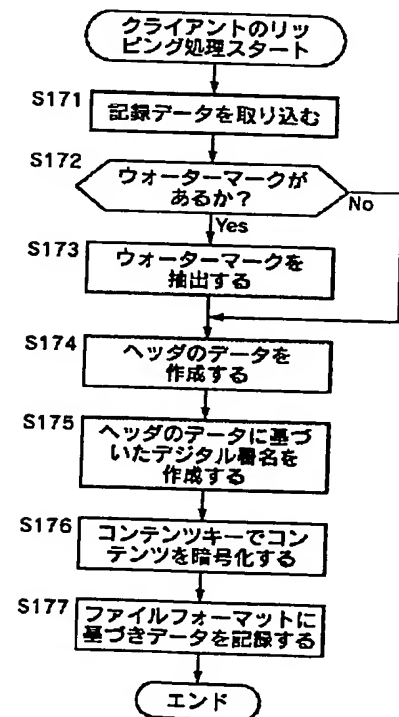
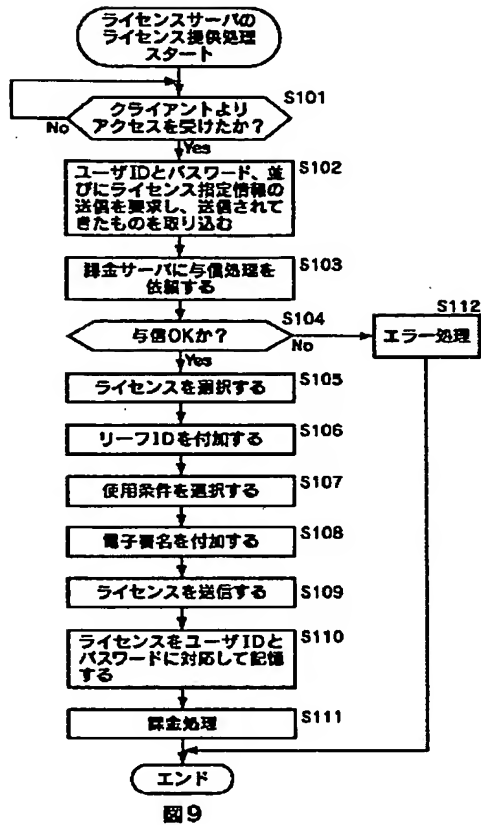
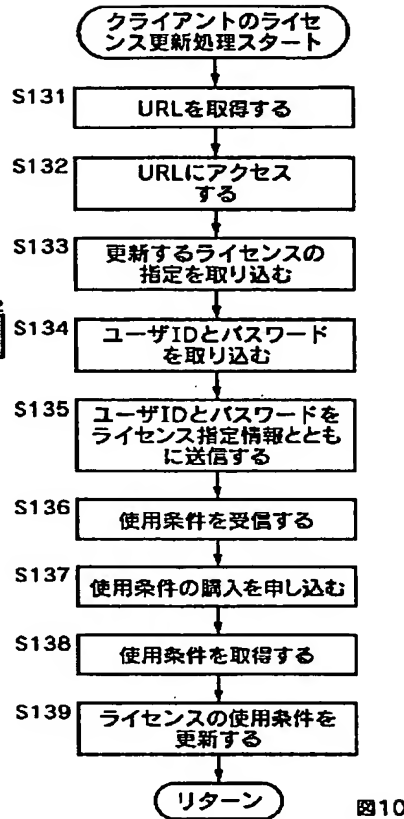


図23

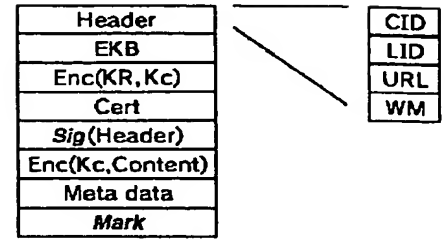
【図9】



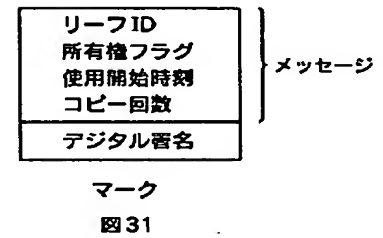
【図10】



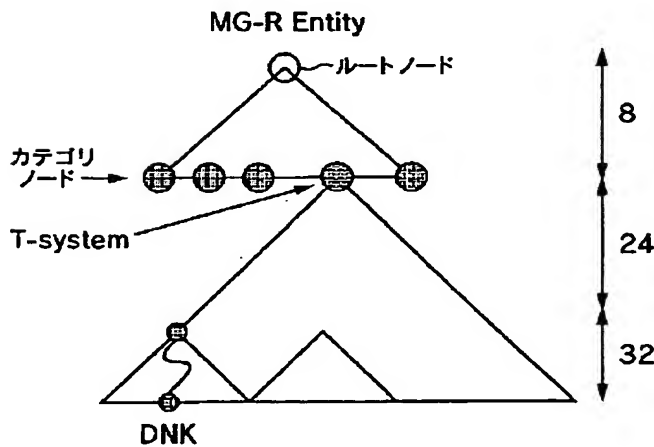
【図25】



【図31】



【図13】



【図34】

Mark = { LeafID, Own, Sig<sub>s</sub>(LeafID, Own) }

図34

【図15】

A 有効化キーブロック(EKB:Enabling Key Block)  
デバイス0,1,2にバージョン:tのノードキーを送付

バージョン (Version) : t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

B 有効化キーブロック(EKB:Enabling Key Block)  
デバイス0,1,2にバージョン:tのノードキーを送付

バージョン (Version) : t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

図15

【図14】

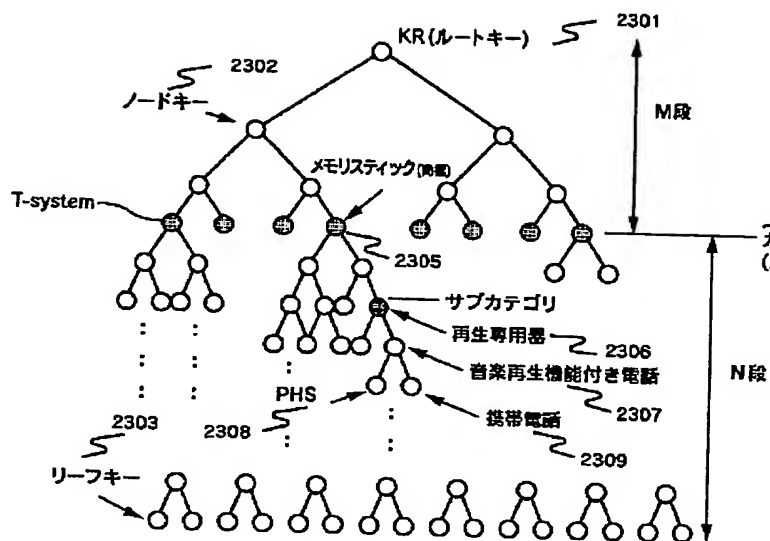


図14

【図16】

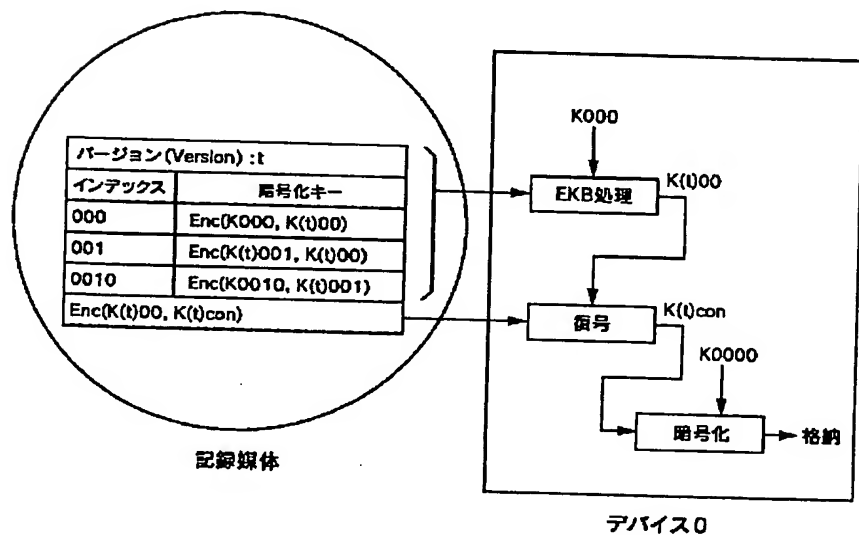


図16

【図39】

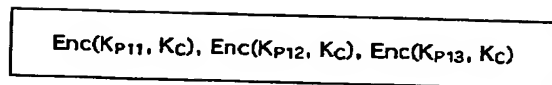


図39

【図33】

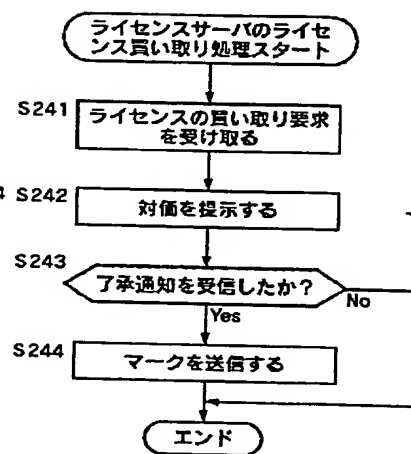


図33

【図35】

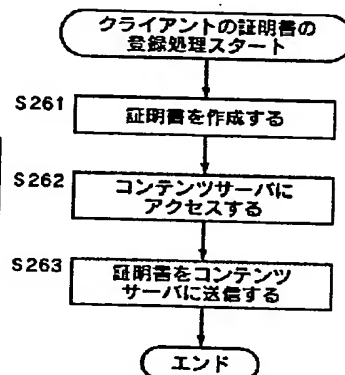


図35

【図36】

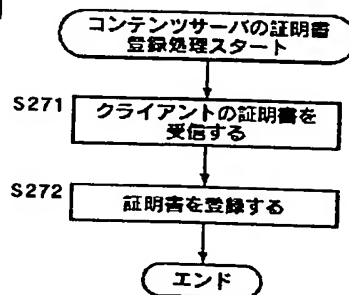
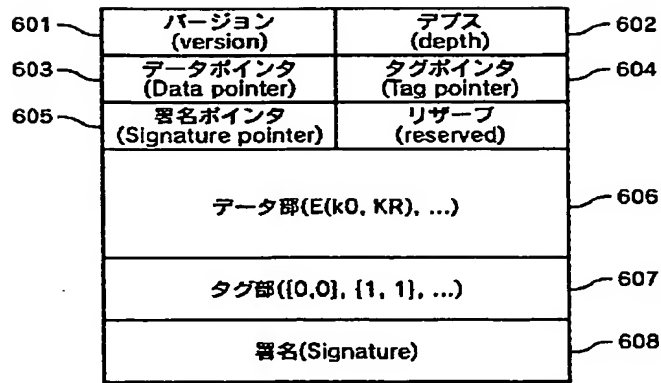


図36

【図17】



EKB

図17

【図19】

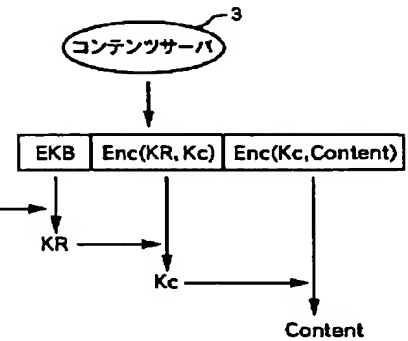


図19

【図18】

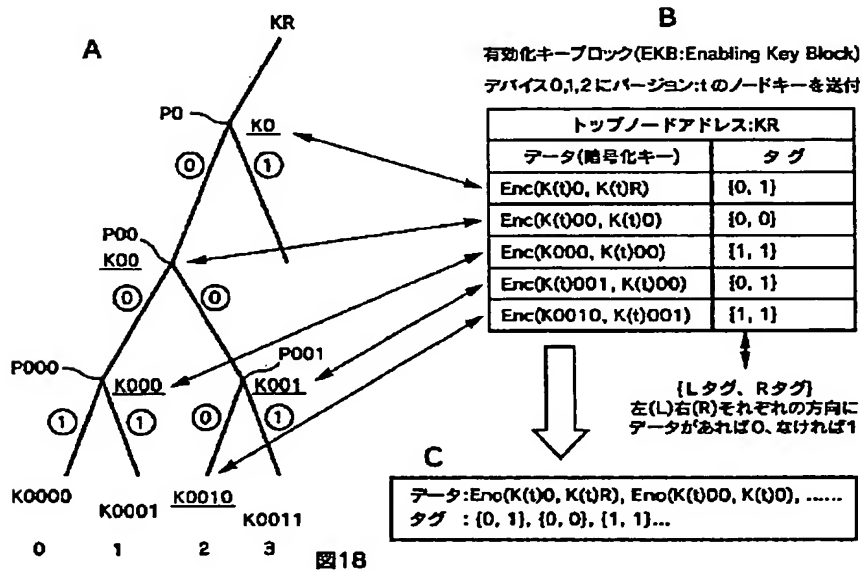


図18

【図37】

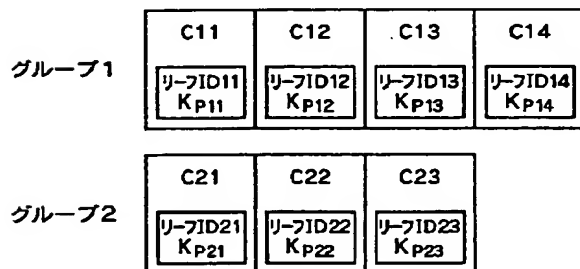


図37

【図40】

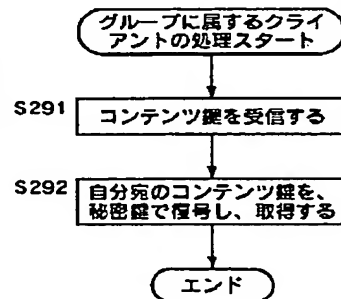


図40

【図38】

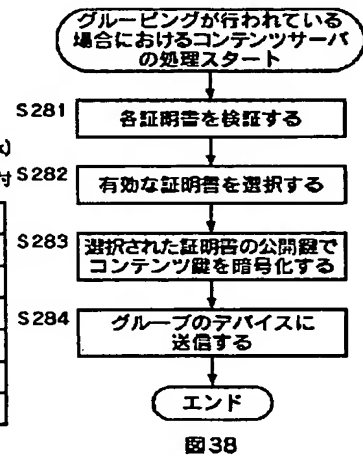


図38

【図42】

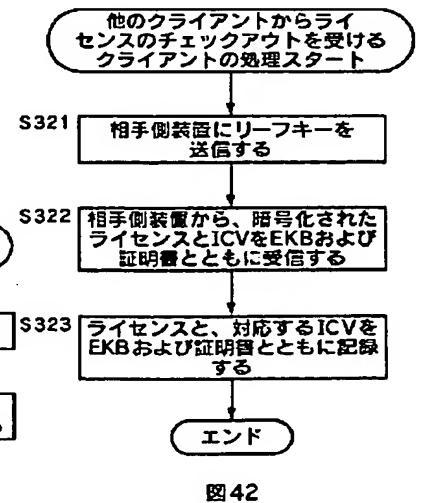
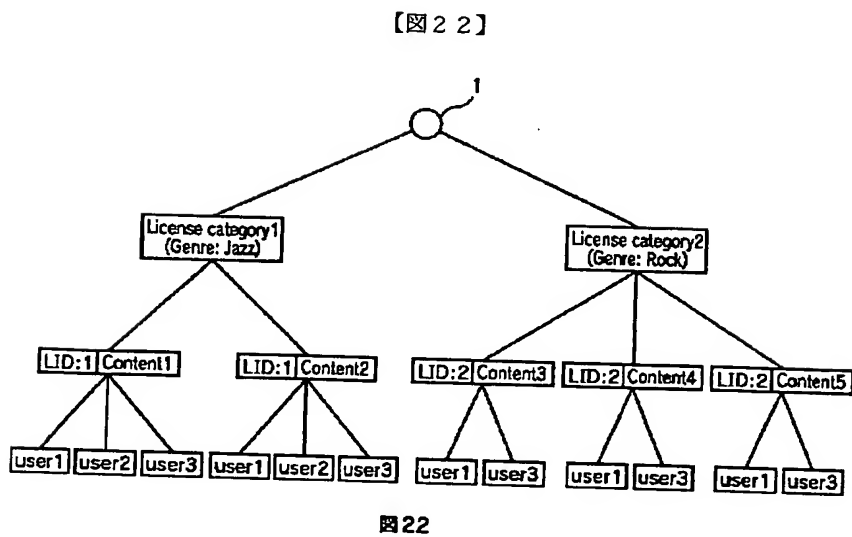
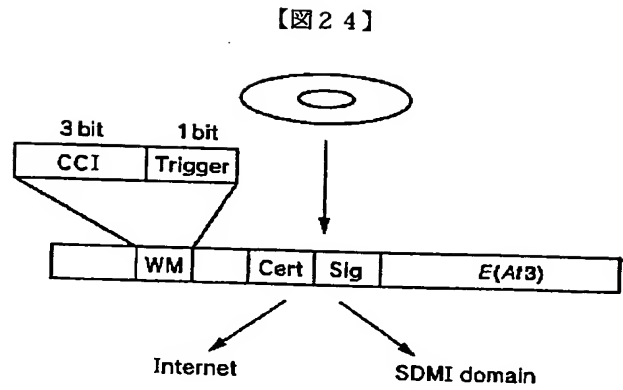
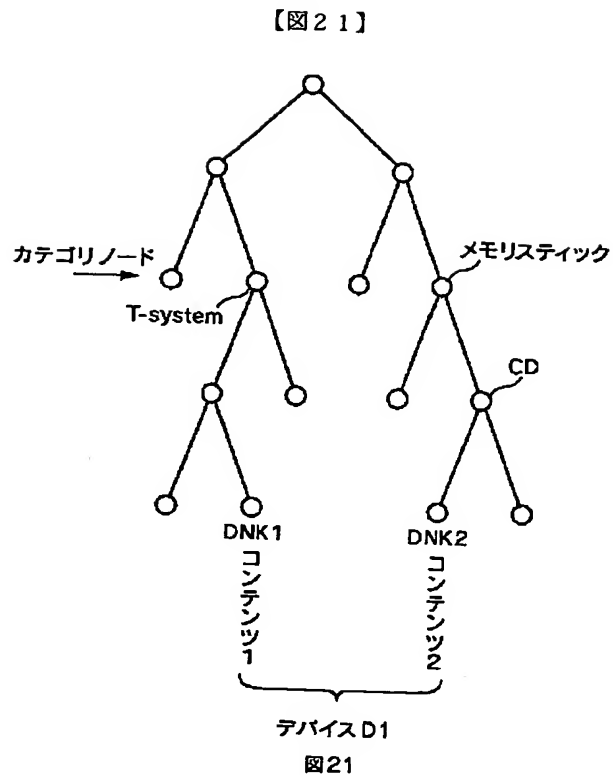


図42



【図26】

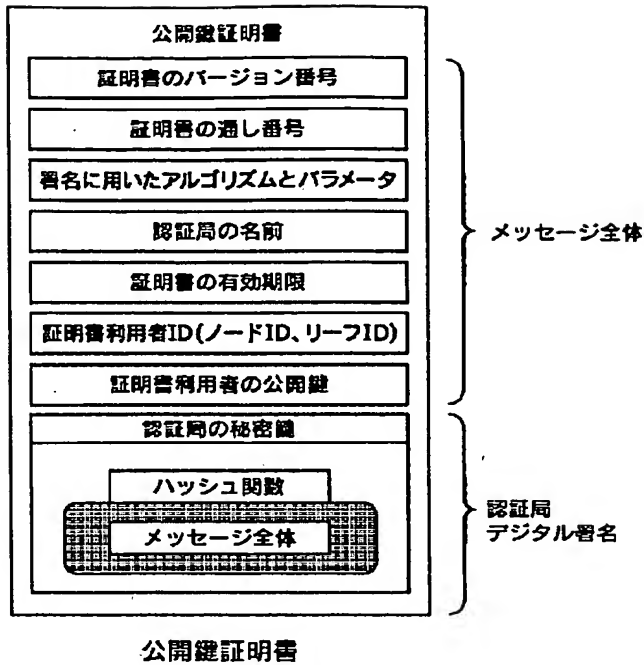


図26

【図29】

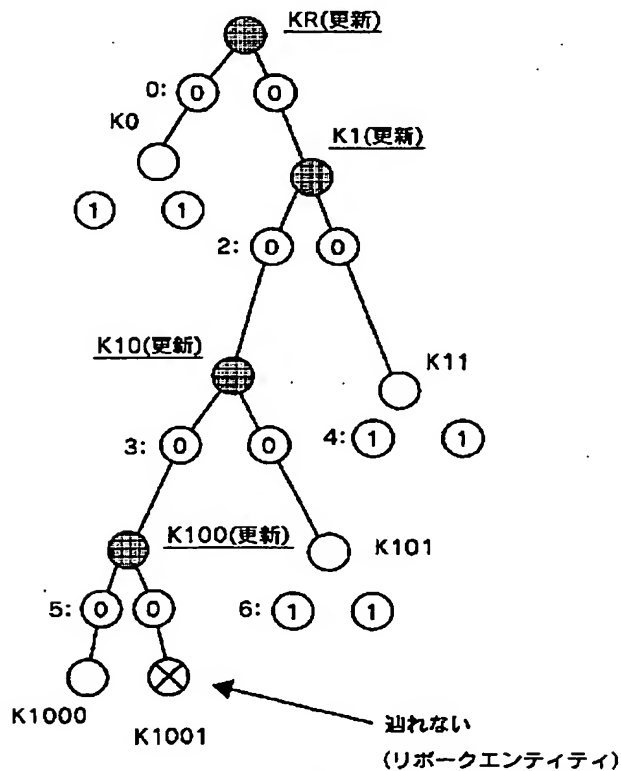


図29

【図27】

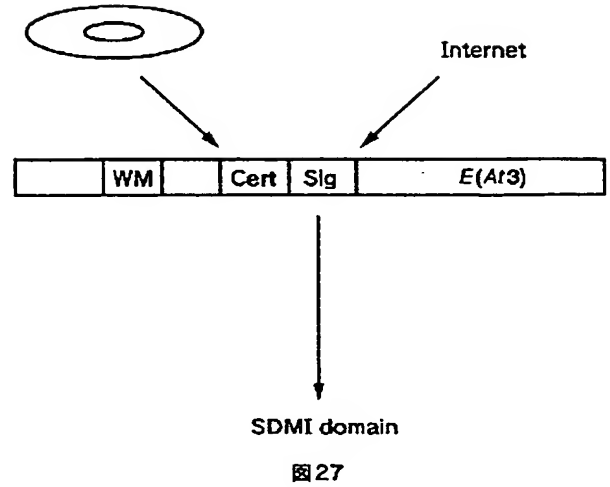


図27

【図28】

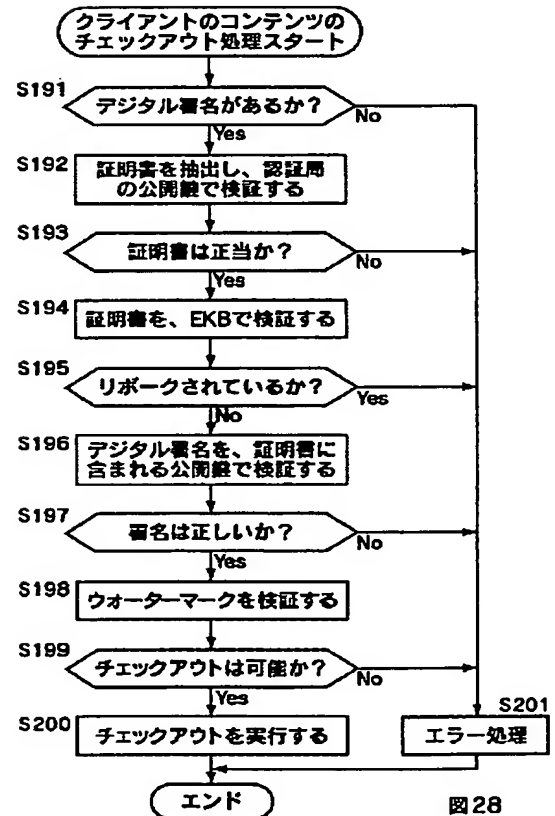


図28

【図30】

有効化キーブロック(EKB:Enabling Key Block)の  
データ部およびタグ

データ (暗号化キー)	Enc(K0, K(t)R), Enc(K(t)1, K(t)R) Enc(K(t)10, K(t)1), Enc(K11, K(t)1) Enc(K(t)100, K(t)10), Enc(K101, K(t)10) Enc(K1000, K(t)100)
タグ	0: {0, 0}, 1: {1, 1}, 2: {0, 0}, 3: {0, 0} 4: {1, 1}, 5: {0, 1}, 6: {1, 1}

{Lタグ, Rタグ}  
左(L)右(R)それぞれの方向に  
データがあれば0、なければ1

図30

【図32】

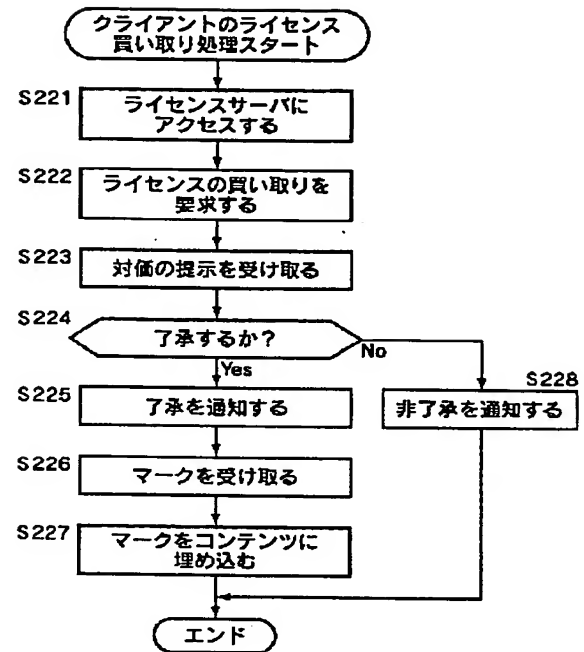


図32

【図41】

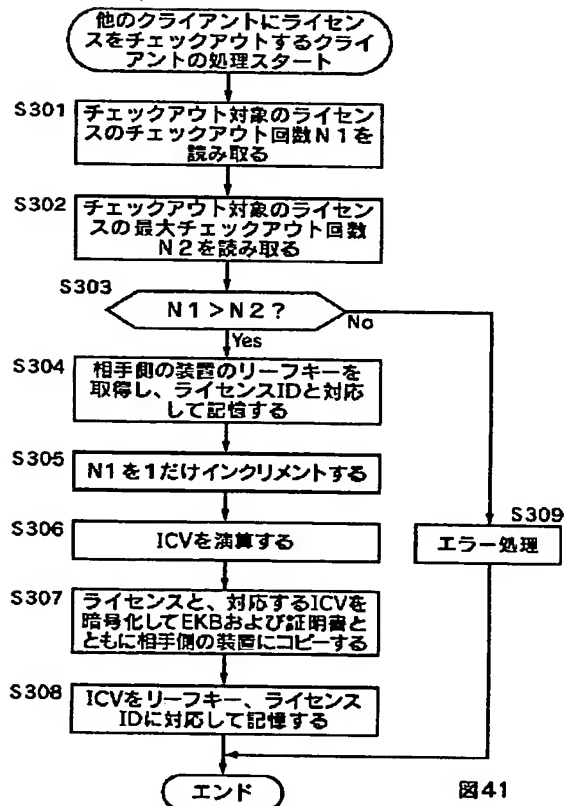


図41

【図43】

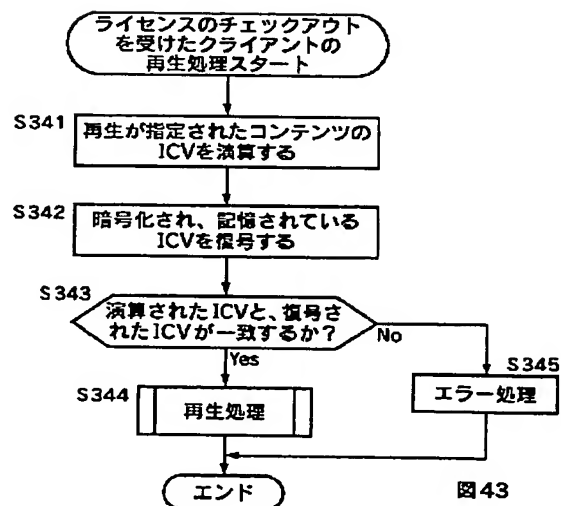


図43

【図44】

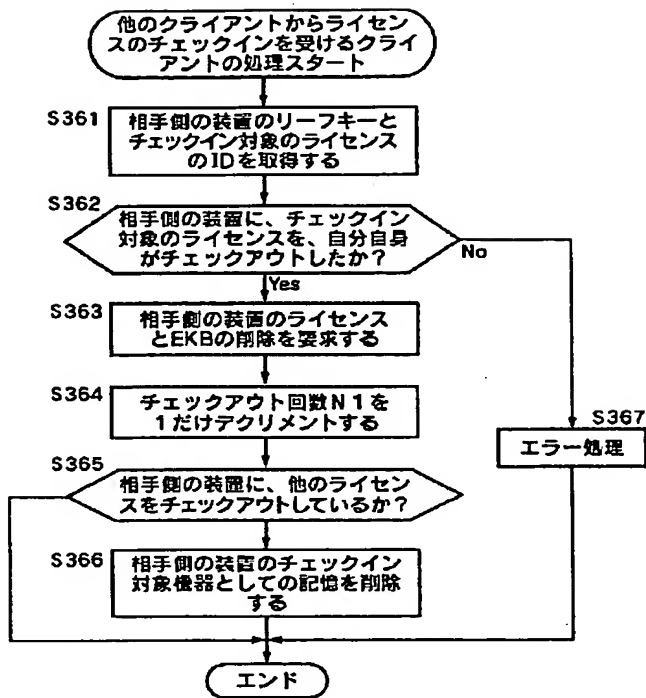


図44

【図45】

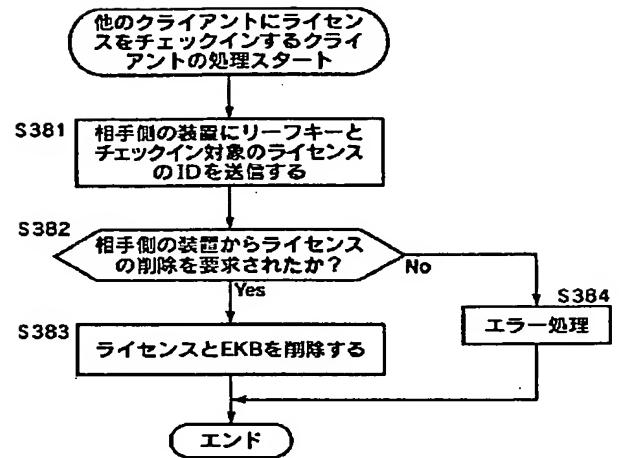


図45

【図46】

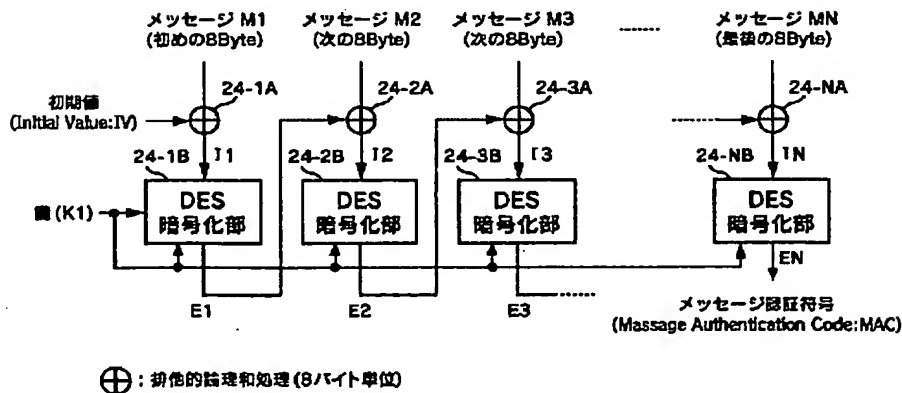


図46

【図47】

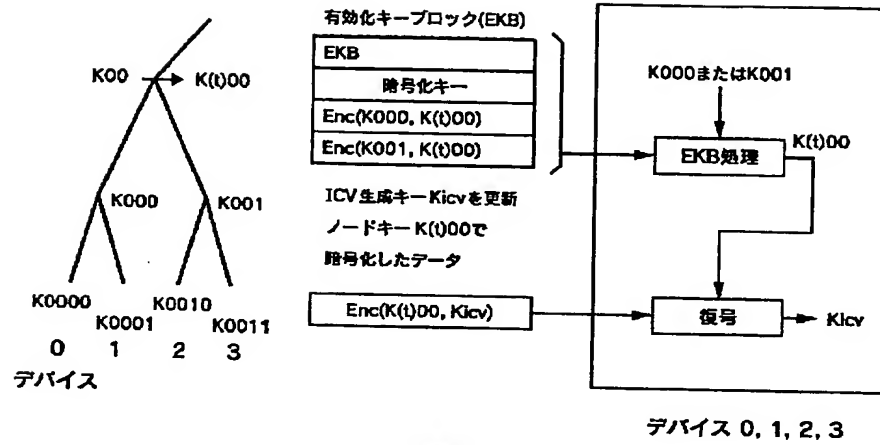


図47

【図48】

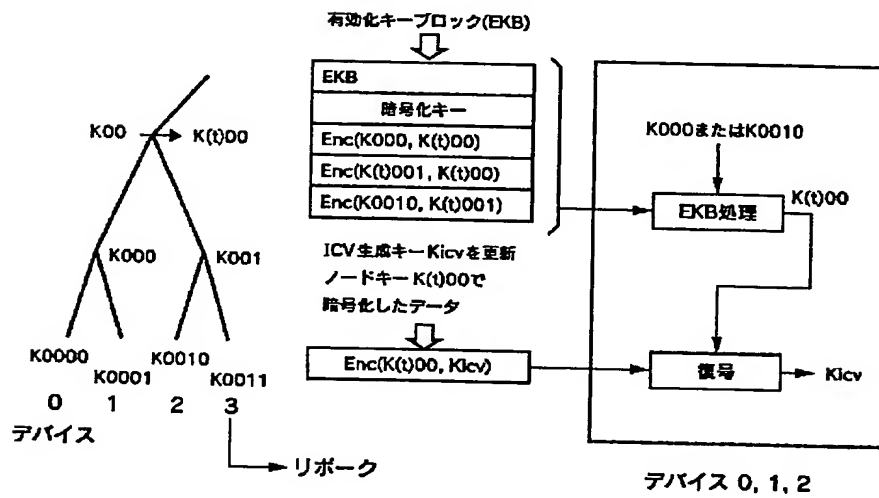


図48

【図50】

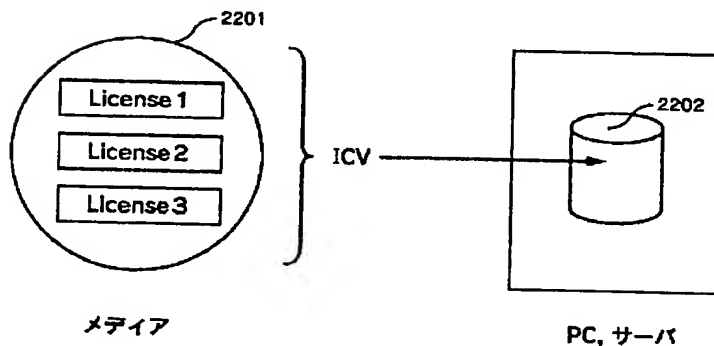


図50

【図49】

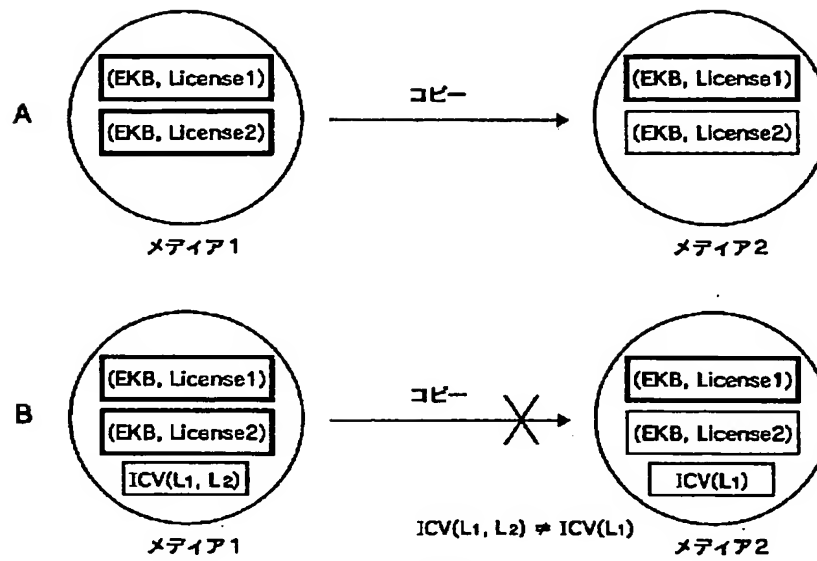


図49

フロントページの続き

(72)発明者 黒田 壽祐  
東京都品川区北品川6丁目7番35号 ソニ  
ー株式会社内

(72)発明者 石黒 隆二  
東京都品川区北品川6丁目7番35号 ソニ  
ー株式会社内  
Fターム(参考) 5J104 AA12 MA05 PA07 PA10

**THIS PAGE BLANK (USPTO)**

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

**THIS PAGE BLANK (USPTO)**